CENTRO FEDERAL

DE EDUCAÇÃO

TECNOLÓGICA DO CEARÁ

Departamento de Ensino
Curso de Telemática

Prof. Dr. Pedro Klécius

Apostilha de Redes Celulares

Índice

Unidade 1 Comunicações Móveis 1-5
1.1 Historia da Telefonia Celular 1-5
1.1.1 1G - redes analógicas de telefonia móvel 1-6
1.1.2 2G (redes digitais de telefonia móvel) 1-6
1.1.2.1 Tecnologia TDMA 1-7
1.1.2.2 Tecnologia CDMA 1-7
1.1.2.3 Tecnologia GSM 1-7
1.1.3 2,5G 1-8
1.1.4 3G (redes de altíssima velocidade) 1-8
1.1.5 4G - quarta geração de telefonia móvel 1-9
Unidade 2 Conceitos celulares 2-10
2.1 Redes celulares 2-10
2.2 Interface rádio 2-10
2.3 Roaming e handover 2-11
2.4 Cobertura Celular 2-11
2.5 Reutilização das freqüências 2-13
2.6 Conceitos de Transmissão 2-13
2.6.1 Ocupação do espectro 2-14
2.6.2 Técnicas de utilização de freqüências: 2-14
2.6.2.1 FDMA = Frequency Division Multiple Acces 2-14
2.6.2.2 TDMA = Time Division Multiple Access 2-15
2.7 PLMN - Rede celular 2-15
Unidade 3 Redes Celulares GSM 3-18
3.1 Histórico do GSM 3-18
3.2 Características do GSM 3-18
3.2.1 Identificação do usuário 3-19
3.2.2 Classificação dos serviços 3-19
3.2.3 Serviços suporte 3-20
3.2.4 Tele-serviços 3-20
3.2.5 Serviços suplementares 3-21
Unidade 4 Arquitetura das Redes GSM 4-22
4.1 Base Station System 4-22
4.1.1 BTS - Base Transceiver Station 4-22
4.1.2 Funções da BTS 4-23
4.1.3 Capacidade de uma BTS 4-23
4.1.4 Potência de uma BTS 4-23
4.1.5 Configuração das BTS 4-24
4.1.6 BSC - Base Station Controller 4-24
4.2 Subsistema Rede 4-25
4.2.1 HLR – Home Localization Register 4-25
4.2.2 MSC/VLR – Móbile Switching Center/Visitor Localization Register 4-25
4.3 Subsistema de operação e manutenção 4-26
4.3.1 Administração da rede 4-26
4.3.2 Arquitetura do TMN 4-26
4.3.3 EIR – Equipment Identity Register 4-26
4.3.4 AUC – AUtentication Center 4-26
4.4 As Interfaces GSM 4-27
4.5 As camadas de Protocolo 4-28
4.5.1 Camadas de protocolo na BSS 4-28

4.6 O terminal móvel 4-29
Unidade 5 Redes Celulares GSM 5-31
5.1 Gerência do Roaming e da Segurança 5-31
5.2 Numeração e identificação 5-31
5.2.1 IMSI - International Móbile Subscriber Identity 5-31
5.2.2 TMSI - Temporary Móbile Subscriber Identity 5-32
5.2.3 MSISDN - Mobile Station ISDN Number 5-32
5.2.4 MSRN - Mobile Station Roaming Number 5-33
5.2.5 IMEI – International Mobile Equipment Identify 5-33
5.3 Autenticação e criptagem 5-34
5.3.1 Confidencialidade do IMSI 5-34
5.3.2 Autenticação e criptagem 5-34
5.3.3 Autenticação do usuário 5-35
5.3.4 Confidencialidade dos Dados 5-35
5.3.5 Gerência dos dados de segurança 5-36
5.4 Gerência da localização (roaming) 5-37
5.4.1 Localização no GSM 5-38
5.4.2 Base de dados de localização no GSM 5-38
5.4.3 Atualização da Localização no GSM 5-38
5.4.3.1 Atualização periódica: 5-39
5.4.3.2 Procedimento IMSI Attach/Detach: 5-39
5.4.3.3 Procedimento de atualização da localização inter VLR 5-40
5.4.3.4 Procedimento de atualização da localização intra VLR 5-40
5.4.3.5 Atualização da localização Internacional 5-41
5.4.4 Atualização devido à mudança de célula 5-42
5.4.4.1 Mudança de célula dentro da mesma LA. 5-42
5.4.4.2 Mudança de célula e de LA. 5-42
5.4.4.3 Mudança de célula e de zona de comutação 5-43
5.5 Tipos de chamada 5-44
5.5.1 Chamadas entre fixo e celular 5-44
5.5.2 Chamadas entre Celulares 5-46
5.6 Handover 5-47
5.6.1 Handover intra BSC 5-47
5.6.2 Handover intra MSC 5-48
5.6.3 Handover inter MSC 5-49
Unidade 6 A interface rádio GSM 6-50
6.1 Compartilhamento de recursos rádio 6-50
6.1.1 Compartilhamento em freqüência 6-50
6.1.2 Compartilhamento em tempo 6-50
6.1.3 Salto de freqüência 6-51
6.1.4 Canal físico duplex 6-51
6.1.5 Numeração das portadoras 6-52
6.1.6 Compensação do tempo de propagação 6-52
6.1.7 Transmissão da voz 6-53
6.1.8 Transmissão de dados 6-53
6.1.9 Modulação GMSK 6-53
6.1.10 Formato do burst 6-54
Unidade 7 Canais Lógicos 7-57
7.1 Estrutura da interface rádio 7-57
7.2 Canais físicos e lógicos 7-57
7.3 Estrutura temporal da multitrama 7-58

7.4 Classificação dos canais lógicos 7-59
7.5 Canais dedicados 7-59
7.5.1 TCH e SDCCH 7-59
7.5.2 Canal SACCH 7-60
7.5.3 Multiplexagem TCH-SACCH 7-60
7.5.4 Multiplexagem SDCH-SACCH 7-60
7.6 Canais não dedicados 7-61
7.6.1 O conceito de canal baliza 7-61
7.6.2 Canal FCCH 7-62
7.6.3 Canal SCH 7-62
7.6.3.1 Estrutura do burst 7-62
7.6.3.2 Colocação do SCH na trama TDMA 7-63
7.6.3.3 Sincronização fina 7-63
7.6.3.4 Dados transportados 7-63
7.6.3.5 Sincronização Lógica 7-63
7.6.3.6 Código de cores BSIC (Base Station Identity Code) 7-63
7.6.4 Canal BCCH 7-64
7.6.5 Canal AGCH 7-64
7.6.6 Canal PCH 7-64
7.6.7 Canal RACH 7-65
7.7 Monitoramento 7-65
7.7.1 Monitoramento nas multitramas a 26 e a 51 7-66
7.8 Hypertrama 7-66
7.8.1 Características dos Canais GSM 7-67

Unidade 1 Comunicações Móveis

1.1 Historia da Telefonia Celular

O uso dos sistemas de radiodifusão foi empregado pela primeira vez em fase experimental durante a 1ª guerra mundial. Motivados pela experimentação, o departamento de polícia de Detroit fez o primeiro uso de sistemas de rádio-móvel operando em 2 MHz, para enviar ordens da Central de Polícia para as viaturas. Em 1932, já dispondo de 11 canais de voz para serem compartilhados por até 5.000 veículos, o departamento de polícia de Nova York, usou esse sistema centralizado baseado na idéia de uma única torre com repetidores e reforçadores de sinal transmitindo os sinais para toda uma grande área onde haveria o serviço.

Posteriormente, devido o surgimento da necessidade de comunicação de empresas com seus funcionários foi imprescindível a criação de um sistema que possibilitasse a comunicação telefônica por rádio. Em meados de 1940, em Saint Louis, nos Estados Unidos, foi implementado o primeiro serviço comercial de telefonia móvel, o qual consistia de um sistema rudimentar com um monofone especialmente desenvolvido, não possibilitando a discagem, que era efetuada por uma operadora.

Em 1946, a FCC (Federal Communication Commission), órgão que regulamenta padrões em telecomunicações nos EUA, permite que a AT&T coloque em operação o primeiro sistema de telefonia móvel. A conexão era manual entre o sistema de rádio e a rede de telefonia pública. Batizado como rádio urbano, era baseado em uma única antena de transmissão de alta potência, que cobria uma área de cerca de 80 Km de raio e operava com apenas três canais funcionando em FM.

No ano de 1947, foi apresentado pela empresa Bell Labs o conceito de telefonia móvel celular. A arquitetura do sistema celular permite a utilização do mesmo canal de rádio em localidades diferentes. Vários usuários utilizam simultaneamente o mesmo canal de rádio multiplicando-se a capacidade de tráfego, técnica denominada de "Reutilização de Freqüência".

Os sistemas de comunicações móveis pioneiros da década de 30 possuíam equipamentos volumosos, pesados, caros e de grande consumo. Os transmissores operavam com potência alta para cobrir a maior área de serviço possível, com a utilização ineficiente do espectro de freqüência e, em geral, com transmissão via única (somente transmitia ou recebia). Em meados de 1950 surgiram os primeiros equipamentos transportáveis pelo homem, mas sua utilização ainda limitava-se às aplicações militares.

Em 1957, com o surgimento dos transistores houve uma grande redução do volume dos aparelhos, em até mais de 50% de seu volume. Isto representou diretamente uma redução de custo, calor dissipado e menor consumo de potência. Os telefones sem fio e telefones celulares portáteis surgiram com a tecnologia VLSI (Very Large Scale Integration) de integração de circuito em larga escala em 1970. Com o avanço tecnológico da década de 80 proporcionado pelas centrais CPA (centrais programáveis), técnicas de sinalização por canal comum e os enlaces digitais, via rádio ou cabo ótico tornou o sistema móvel celular mais barato ao usuário.

Nos últimos anos, os sistemas móveis celulares se popularizaram mundialmente, principalmente devido à tecnologia ULSI (Ultra Large Scale Integration). A tecnologia celular tem evoluído de analógica para digital, objetivando a eficiência do espectro, qualidade de voz e integração de serviços. A gama de novas possibilidades embutidas nos celulares, tais como acesso a filmes, informativos, câmera de foto e vídeo, somente se tornou possível graças a esse avanço tecnológico que o setor vem atravessando. Com a alta tecnologia, o diferencial entre as empresas será então, a qualidade de atendimento e a capacidade de ter os melhores produtos e serviços com os preços mais competitivos.

Podemos classificar as redes celulares em gerações da seguinte maneira:

1G (primeira geração) - redes celulares analógicas;

2G (segunda geração) - redes celulares digitais baseadas em comutadores de circuitos: redes CDMA, TDMA e GSM que nós conhecemos;

2,5G – redes 2G com transmissão de pacotes de média/alta velocidade, voltados para transmissão de dados. GPRS e EDGE nas redes GSM, 1xRTT nas redes CDMA.

3G - redes de altíssima velocidade, com possibilidades de streaming de vídeo, videoconferência, transmissões em tempo real, jogos online. Em alguns países, já existe o 3G, com as licenças UMTS.

1.1.1 1G - redes analógicas de telefonia móvel.

A primeira geração de telefonia móvel, apelidada 1G, utilizava a modulação de sinais analógicos em uma portadora de RF e operava sobre redes com tecnologia de comutação de circuito. Neste tipo de rede, um circuito de voz é alocado permanentemente enquanto dura a chamada. Trata-se de um serviço orientado a conexão. O acesso à canalização é obtido através do método FDMA (Frequency Division Multiple Access). Essa tecnologia é limitada quanto ao número possível de usuários, pois admite apenas uma "ligação" por canal, o que, rapidamente exaure a capacidade de cada ERB, obrigando a instalação de uma maior quantidade de células.

O tamanho das células situa-se na faixa de 500 metros a 10 quilômetros, sendo permitido o "handoff" ou "handover" (transferência automática de ligações de uma célula para outra). Possibilita igualmente o "roaming" (transferência automática de ligações entre sistemas) entre os diferentes provedores de serviço, desde que adotem o mesmo sistema.

O primeiro sistema celular dos EUA entrou em operação comercial em Chicago em 13 de Outubro de 1983. Esse sistema celular de alta capacidade ficou conhecido pela sigla AMPS, ou seja, Advanced Mobile Phone Service. No entanto, a NTT (Nippon Telephone & Telegraph) havia se antecipado colocando um sistema semelhante ao AMPS em operação em 1979 na cidade de Tóquio, no Japão.

Na Europa a primeira geração de sistemas celulares era composta de diversos sistemas. O NMT (Nordic Mobile Telecommunications), adotado por diversos paises nórdicos, o TACS (Total Access Communications System), no Reino Unido, Itália, Áustria, Espanha e Irlanda, o C-450 na Alemanha e Portugal, o Radiocom 2000 na França e o RTMS na Itália. Todos esses sistemas eram bastante parecidos entre si, sendo que as principais diferenças concentravam-se no uso do espectro de freqüência e no espaçamento entre canais. O AMPS opera na faixa de 869-894 MHz para recepção e 824-849 MHz para transmissão; o NMT-450 opera na faixa de 463-468 MHz para recepção e 453-458 MHz para transmissão enquanto que o NMT-900 utiliza a faixa de 935-960 MHz para recepção e 890-915 MHz para transmissão, etc. Com relação ao espaçamento entre os canais pode-se citar o AMPS que adota 30 kHz, o TACS e vários outros que adotam 25 kHz.

O AMPS (Advanced Mobile Phone Service) foi o primeiro sistema de telefonia móvel celular adotado no Brasil, no Rio de Janeiro, em 1991.

1.1.2 2G (redes digitais de telefonia móvel)

Com a demanda de novos usuários, o sistema de telefonia analógico foi rapidamente exaurido. Novos sistemas com novas tecnologias seriam necessários. Assim surgiu a segunda geração de redes celulares ou 2G. Na 2G, um sinal digital é modulado na RF. Entretanto o sinal digital modulado é ainda transportado sobre redes com tecnologia comutada a circuito, assim como no 1G. Algumas vantagens imediatas do sistema 2G sobre o 1G foram: a acomodação de maior número de usuários numa mesma faixa de freqüência, possibilidade de conferência entre usuários e sistema de mensagens de voz e texto.

Com o 2G, o FDMA é ainda usado para a divisão da faixa de freqüência em pequenos blocos, porém a utilização de tais blocos é feita com a adoção de duas novas tecnologias de acesso digital: TDMA (time division multiple Access) e CDMA (code division multiple Access). Estas tecnologias são classificadas como "air interface": uma forma de manipular os sinais de

forma a maximizar o uso da faixa de freqüência disponível. Serviços 2G "puros" podem ofertar uma taxa de transmissão de dados de até 14 Kbps.

1.1.2.1 Tecnologia TDMA

A sigla TDMA vem do inglês Time Division Multiple Access , que quer dizer "Acesso Múltiplo por Divisão de Tempo". O TDMA é uma técnica de acesso que funciona dividindo um canal de freqüência em vários intervalos de tempo distintos. Cada usuário ocupa um espaço de tempo específico na transmissão, o que impede problemas de interferência.

No sistema celular também chamado TDMA um canal de voz utiliza um par de canais: um chamado direto (para comunicação no sentido antena – dispositivo móvel) e outro reverso (no sentido dispositivo móvel – antena), ambos de largura de 30 KHz e distância entre eles de 45 MHz (separação full-duplex). Originalmente, o sistema celular trabalhava com 666 pares de canais em uma faixa de freqüência de 825 MHz a 845 MHz para canais diretos e 870 MHz a 890 MHz para canais reversos, sendo que os primeiros 333 eram os canais denominados banda A e os acima de 334 os de banda B. Posteriormente, em 1986, o sistema se expandiu e novos canais foram adicionados às bandas A e B.

As bandas A e B são utilizadas por operadoras diferentes. No Brasil, determinou-se que a banda A seria usada por operadoras estatais do sistema Telebrás e a banda B para operadoras privadas. Cabia a operadora determinar qual tipo de "air interface" adotaria para montar sua rede de acesso digital, se TDMA ou se CDMA.

1.1.2.2 Tecnologia CDMA

A sigla CDMA vem do inglês Code Division Multiple Access , que quer dizer "Acesso Múltiplo por Divisão de Código". O CDMA é uma tecnologia de acesso digital que funciona transformando a voz ou dados do usuário em um sinal da rádio codificado, que é recebido pelas antenas e transformado novamente para o receptor.

Em termos de redes operacionais atualmente, o TDMA e variantes estão na liderança sobre o CDMA. O TDMA é utilizado nos EUA e tem representação no Japão com o Japanese Digital Cellular, JDC. No Brasil, a maioria das operadoras preferiu o TDMA. A ATL presta serviço TDMA no Rio de Janeiro e Espírito Santo utilizando a banda B enquanto a Telefônica Celular presta serviço CDMA na mesma área utilizando a banda A. Em São Paulo a Telesp presta serviço CDMA na banda A; a antiga BCP Telecomunicações, na banda B, serviço TDMA na capital; e a TESS presta serviço TDMA na banda B em Campinas e interior. Em Minas Gerais a Telemig Celular presta serviço TDMA na banda A e a Maxitel, também TDMA na banda B. Os primeiros terminais digitais no Brasil foram ativados em 1998.

1.1.2.3 Tecnologia GSM

A sigla GSM vem do inglês Global System for Mobile Communications, que quer dizer "Sistema Global para Comunicações Móveis". O GSM é um sistema de celular digital baseado em divisão de tempo, como o TDMA, e é considerada a evolução deste sistema, pois permite, entre outras coisas, a troca dos dados do usuário entre aparelhos telefônicos através do Sim-Card e acesso mais rápido a serviços WAP e Internet.

A tecnologia GSM é utilizada como padrão para telefonia celular digital na Europa desde 1992 e está presente nas Américas desde 1983. Por isto é o sistema celular de maior cobertura em todo o mundo. Apesar disto, por se tratar de uma tecnologia ainda recente no Brasil, sua abrangência nacional ainda não tem o mesmo alcance das demais operadoras já instaladas, o que deve ser resolvido em pouco tempo.

Algum tempo depois de definir o uso das bandas A e B no Brasil, a Anatel, Agência Nacional de Telecomunicações, divulgou a faixa de freqüência para a nova Banda C, que é de 1,8 GHz, utilizando o padrão GSM.

1.1.3 2,5G

Um novo degrau da evolução do padrão 2G foi sua integração com transmissão de pacotes de dados, devido a forte demanda de serviços de acesso à internet para ambiente wireless. Esta nova capacidade recebeu o nome de sistemas 2,5G. O maior incremento que o 2,5G trouxe foi uma técnica avançada de modulação (comparado ao 2G), permitindo a comutação de pacotes ao invés de circuitos, a mesma técnica de transmissão adotada pelo IP da arquitetura TCP/IP. Diferentemente da comutação por circuito que aloca um circuito fim-a-fim durante a transmissão, a comutação de pacotes só utiliza o caminho quando de fato há dados para transmitir. Assim, a tecnologia 2,5G trouxe um uso mais eficiente do espectro de freqüência e da banda disponível, promovendo o meio de transporte mais apropriado para a navegação de aplicações na internet a partir de dispositivos wireless, notadamente com o surgimento de aparelhos celulares com esta capacidade. Com 2,5G puro, pode-se atingir a taxa de transmissão de dados de até 144 Kbps.

Na maioria dos casos, os sistemas 2,5G são implementados diretamente sobre as redes 2G existentes. Como resultado, um sistema 2,5G não é uma rede comutada a pacotes "pura". Na verdade, pacotes de dados são transmitidos sobre redes de circuitos comutados. Redes wireless comutadas puras a pacote só serão mesmo disponibilizadas com o advento da geração 3G. Formalmente, as redes digitais hoje em operação no Brasil (TDMA, CDMA e GSM) são da geração 2G. O 2,5G será alcançado com a inclusão do protocolo GPRS, General Packet Radio Services, sobre redes GSM.

Uma segunda evolução para redes 2G, após o GPRS, é a técnica de modulação denominada EDGE, Enhanced Data GSM Environment. Enquanto GPRS utiliza a modulação GMSK, EDGE utiliza a 8 PSK que possibilita um incremento na velocidade de transmissão de três vezes sobre o GPRS.

1.1.4 3G (redes de altíssima velocidade)

Mesmo não estando ainda os sistemas de segunda geração totalmente amadurecidos e firmemente estabelecidos, já se trabalha intensamente no desenvolvimento da terceira geração. Este trabalho está sendo liderado mais uma vez pela Europa e patrocinado pelo ITUR (International Telecommunications Union Radiocommunications sector) e ETSI (European Telecommunications Standard Institute). O objetivo é criar um sistema móvel de terceira geração denominado UMTS (Universal Mobile Telecommunications System).

Progressos significativos já foram obtidos, como por exemplo a reserva de 230 MHz de espectro, com a aprovação de 127 países, na "World Administrative Radio Conference" (WARC) em 1992.

A topologia provável desse novo sistema é baseada em uma forma de arquitetura mista de células; células de tamanho variável serão implementadas com dimensionamento adequado para áreas geográficas específicas e em função das diferentes demandas de tráfego. Células diminutas, ou seja, picocélulas, instaladas em interiores, serão versões melhoradas das atuais tecnologias "cordless", com "handsets", isto é, aparelhos de assinante, bastante pequenos e leves; células maiores, ou seja, microcélulas e macrocélulas, poderão operar segundo características evoluídas a partir do GSM. "Handsets" diferentes precisarão reconhecer e operar indistintamente em pico, micro e macrocélulas. Ou seja, o objetivo é criar uma plataforma de rede sem fio, oferecendo aos usuários a possibilidade de acesso, através de ondas de rádio, como extensão do sistema telefônico do escritório quando se encontram no trabalho ou como telefone móvel convencional quando se encontram ausentes ou ainda como telefone principal de suas residências quando estão em casa.

A evolução em direção aos serviços de telecomunicações móveis universais, UMTS, muito provavelmente, deverá ter como base a estrutura do GSM. Econômica e tecnicamente falando, a criação de um padrão independente para o UMTS seria injustificável dado o enorme investimento para a viabilização das redes celulares digitais já em uso.

O objetivo do UMTS é prover um padrão universal para as comunicações pessoais com o apelo do mercado de massa e com a qualidade de serviços equivalente à rede fixa. Na visão UMTS, um sistema de comunicações deverá suportar diversas facilidades: (1) portadoras realocáveis, banda atribuível sob demanda (por exemplo, 2 Mbps para comunicações em ambientes internos e pelo menos 144 kbps para ambientes externos); (2) variedade de tipos de tráfego compartilhando o mesmo meio; (3) tarifação adequada para aplicações multimídia; (4) serviços personalizados; (5) facilidade de implementação de novos serviços (por exemplo, utilizando ferramentas de rede inteligente); (6) WLL (Wireless Local Loop) de banda larga, etc. O WLL de banda estreita tem sido utilizado em substituição aos fios/cabos de cobre para conectar telefones e outros dispositivos de comunicação com a rede de telefonia comutada pública, ou PSTN (Public Switched Telephone Network).

Os delegados do ETSI reunidos em Paris em 29/01/98 concordaram com a adoção de um padrão de interface aérea para a terceira geração que incorpora elementos de duas tecnologias: W-CDMA (Wideband Code Division Multiple Access) e TDMA/CDMA (híbrido de "Time Division Multiple Access/Code Division Multiple Access"). A rede básica do sistema deverá ter como base o GSM.

O projeto de um produto pessoal como o terminal de assinante para o celular ou PCS vem também se tornando num desafio crescente para a indústria. Os terminais têm se tornado cada vez menores, mais leves, as baterias têm durado mais e os novos modelos que surgem apresentam sempre uma série de novas características e funcionalidades.

A Hewlett-Packard Co. e outros estão tentando concentrar todas as funções de um telefone em um cartão de crédito comum. Os laboratórios de pesquisa da British Telecom, Reino Unido, estão desenvolvendo um comunicador pessoal como peça de vestuário e que combine vídeo, telefonia, comunicação de dados. A Sony vem trabalhando há anos num sistema que efetua traduções em tempo real, de forma que pessoas de países diferentes possam estabelecer uma conversação normal em línguas diferentes. Adicionalmente, todo esse poder de processamento deverá estar concentrado em um único "chip".

A integração da tecnologia de computação com a de comunicações e a eletrônica de estado sólido deve se constituir na base para sistemas multimídia com fantásticos poderes de processamento. Virtualmente, dentro de algum tempo, qualquer indivíduo poderá ter acesso às comunicações sem fio e estará enviando ou recebendo "e-mails", "faxes", vídeo e, na maioria dos casos, utilizando dispositivos portáteis.

Geração	1G	2G	2,5G	3G
Tipo do sinal no acesso	Analógico	Digital	Digital	Digital
Comutação da rede	Circuito	Circuito	Pacote	Pacote
Aplicações disponíveis	Voz	Mensagem	Internet	Multimídia
Taxas de transmissão	---	14 Kbps	144 Kbps	384 Kbps – 2 Mbps
Exemplo de sistema	AMPS	TDMA, CDMA, GSM	GSM + GPRS	UMTS

1.1.5 4G - quarta geração de telefonia móvel

Os celulares 3G ainda não foram lançados, mas a comunidade cientifica já trabalha no desenvolvimento da tecnologia para a quarta geração da telefonia móvel. Pesquisas relacionadas com a 4G prometem taxas de transmissão bem maiores que os antecessores e a possibilidade de exibir filmes em alta qualidade.

Unidade 2 Conceitos celulares

2.1 Redes celulares

Um sistema de comunicações móveis (rede celular) tem por objetivo permitir o acesso ao sistema telefônico a partir de um terminal portátil sobre um território extenso (estado, pais, etc). Esse serviço utiliza uma ligação radioelétrica entre o terminal móvel e a rede. Varias bandas de freqüências podem ser utilizadas tais como as bandas de 450MHz, 900MHz e 1800MHz.

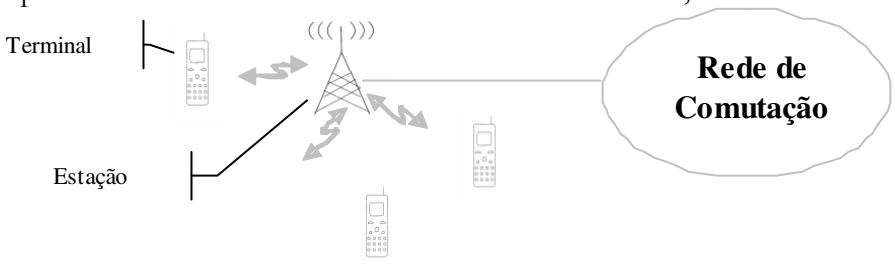


Figura 1 Rede Móvel

Para que o serviço esteja disponível, é necessário que a ligação rádio entre o terminal e a rede seja de qualidade suficiente, o que pode necessitar de uma grande potência de transmissão. A fim de limitar a potência os operadores da rede colocam no território a cobrir um conjunto de estações de base, chamadas BS (Base Station), para que o terminal esteja sempre a menos de alguns km de uma delas.

A área sobre a qual um terminal pode estabelecer uma ligação rádio com uma BS determinada é chamada de **célula**.

Chamamos de estação móvel, ou simplesmente MS (Móbile Station), todo equipamento terminal capaz de se comunicar na rede celular. Uma MS é composta de um emissor-receptor e de uma lógica de controle. Ele pode ser:

- um equipamento instalado num veiculo;
- um equipamento portátil, de pequeno peso e de baixa potência, facilmente transportado.

2.2 Interface rádio

O interesse de uma rede móvel é a mobilidade. A utilização de uma ligação rádio permite cortar o cordão que interliga um telefone ou um microcomputador as redes fixas e os autorizar a se locomover livremente. Entretanto, um meio aéreo possui as características seguintes:

- ele é comum a todos os usuários e difusivo por natureza, seu uso deve ser compartilhado;
- o canal é perturbado por interferência e introduz trajetos múltiplos;
- a característica difusiva do meio aéreo torna possível a escuta indiscreta das conversações telefônicas: torna-se logo necessário a introdução de mecanismos de codificação (criptagem) para garantir a confidencialidade;
- o meio aéreo é raro e caro: as freqüências de rádio são recursos limitados sendo essencial sua economia.
- para utilizar eficazmente o meio aéreo é necessário escolher e colocar em funcionamento técnicas de modulação, codificação e de métodos de acesso.

2.3 Roaming e handover

O usuário de uma rede celular que se desloca em diferentes pontos do território coberto deve poder chamar e ser chamado. Essa noção é chamada de roaming (do inglês to roam ou errar). O roaming é definido como a possibilidade de utilizar o terminal em um ponto qualquer da rede. Esta deve então ser capaz de memorizar a localização do usuário e de lhe encaminhar as chamadas que lhe são destinadas.

Durante uma comunicação o terminal está em comunicação rádio com uma estação de base determinada. Entretanto, devido ao deslocamento do usuário, pode ser necessário trocar a estação de base com a qual o terminal está em comunicação. Essa noção é chamada de transferência intercelular ou handover.

2.4 Cobertura Celular

As redes celulares de primeira geração possuíam células de tamanho grande (50 km de raio) ao centro das quais se situavam as estações transmissoras. No começo, os sistemas alugavam uma banda de freqüências de maneira estática a cada usuário que se encontrava dentro da célula quer ele havia necessidade ou não. Esse sistema só permitia fornecer um serviço a um número de usuário igual ao número de bandas de freqüências disponíveis.

A primeira melhoria consistiu em alugar um canal a um usuário somente a partir do momento que ele havia necessidade permitindo assim aumentar estatisticamente o número de usuários, visto que nem todo mundo telefone ao mesmo tempo.

Mais esse sistema necessitava sempre de estações móveis de grande potência de emissão (8 W) e logo de aparelhos móveis de tamanho e peso consideráveis. Ainda mais, a fim de evitar as interferências, duas células adjacentes não podiam utilizar as mesmas freqüências. Logo, essa organização da rede não utilizava maneira ótima o espectro de freqüência.

Foi para resolver esses diferentes problemas que apareceu o conceito de célula. O principio desse sistema é dividir o território em pequenas zonas, chamadas células, e de repartir as freqüências rádio entre elas.

Assim, cada célula é constituída de uma estação de base (interligada à Rede Telefônica Comutada, RTC) a qual é associado um certo número de canais de freqüência de banda estreita, que são simplesmente chamadas de freqüências.

Como anteriormente, essas freqüências não podem ser utilizadas dentro das células adjacentes a fim de evitar as interferências. Assim, são definidos motivos, também chamados de clusters, constituídos de varias células, dentro dos quais cada freqüência é utilizada uma única vez. A Figura 2 mostra um exemplo de um motivo.

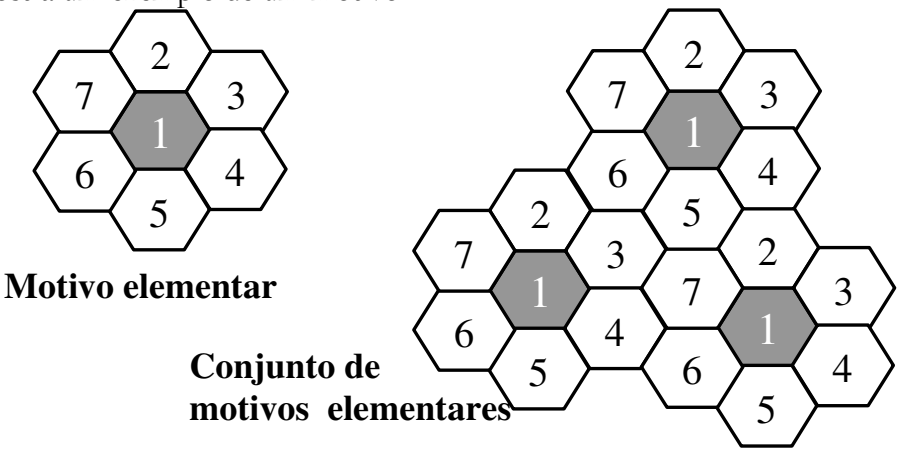


Figura 2 Motivos Celulares

Graficamente uma célula é representada por um hexágono que se aproxima de um circulo. Para permitir ao usuário manter a comunicação no caso dele passar de uma célula para

outra, é necessário que as zonas de cobertura se interponham em 10 a 15 %. Isso reforça o fato das células vizinhas não poderem utilizar uma mesma banda de freqüências.

Para evitar as interferências entre células que utilizam a mesma freqüência é possível fixar a potência de emissão da estação de base em função da distancia que a separa do usuário. O mesmo processo de controle de potência é igualmente aplicado no sentido inverso. De fato, para diminuir a consumação de energia dos telefones celulares e assim aumentar sua autonomia, a potência de emissão é calculada em função da distancia que o separa da estação de base. Graças às medidas efetuadas permanentemente pelo telefone celular e pela estação de base, as potências de emissão são reguladas em permanência para garantir uma qualidade adequada para uma potência mínima. Assim uma célula se caracteriza pela:

- Potência nominal de emissão,
- Freqüência portadora utilizada nas emissões radioelétricas,
- Rede celular a qual ela está interconectada.

As células de um território não possuem todas o mesmo tamanho, pois este depende:

- Do número de usuários potenciais dentro da célula,
- Da configuração do terreno (relevo geográfico, presença de imóveis, etc),
- Da natureza das construções (casas, edifícios, imóveis de cimento armado, etc),
- Da localização (rural, suburbana ou urbana) e da densidade das construções.

Nas zonas rurais onde o número de usuários é pequeno e o terreno é relativamente plano, os operadores utilizam células de tamanho grande (ate 30 Km) e são chamadas de macro-células. No caso de zonas urbanas, onde o número de usuário por unidade de área é considerável e a atenuação devido às construções é muito grande, os operadores utilizam micro-células de algumas centenas de metros de raio. A Figura 3 ilustra o conceito de micro e macro células.

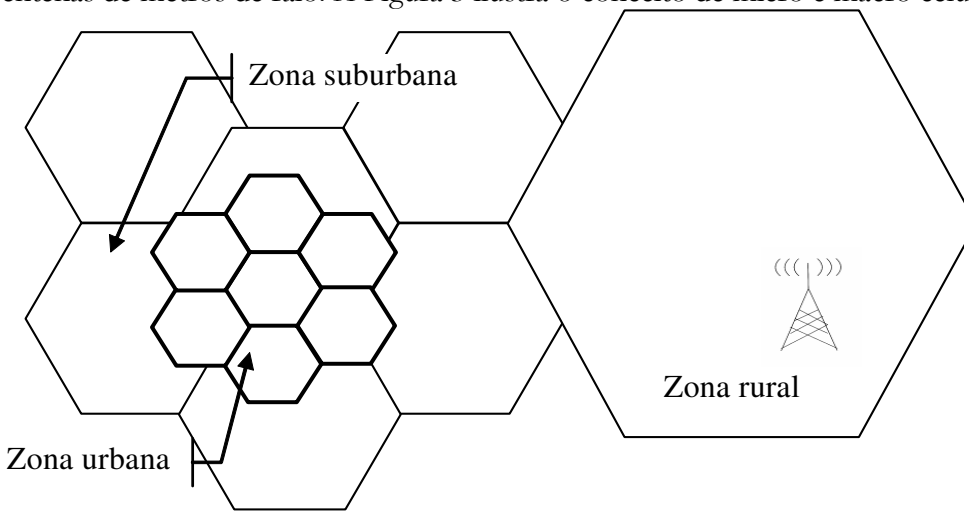


Figura 3 Micro e macro células

Os serviços executados nessas células podem ser classificados em categoria como segue:

1. Serviço « Outdoor » que indica as condições necessárias para o bom desenrolar de uma comunicação no exterior.

2. Serviço « Incar » que toma em conta os usuários que se encontram dentro de automóveis. Nesse caso são tipicamente adicionados uma margem suplementar de 6 décibeis no cálculo de potência .

3. Serviço « Indoor » que permite o bom desenrolar das comunicações no interior dos edifícios. Essa categoria de serviço se subdivide em duas:

(a) « Soft Indoor" quando um usuário de encontra logo atrás de um fachada de um edifício

(b) « Deep Indoor » quando o usuário se encontra mais no interior do edifício.

2.5 Reutilização das freqüências

Sendo as células de tamanho menor, a potência de emissão é mais fraca e o número de usuários por unidade de área pode aumentar. É graças ao principio da reutilização de freqüências que um operador pode aumentar a capacidade da sua rede celular. De fato, basta recortar uma célula em diversas células menores e fazer seu plano de freqüências de forma a evitar as interferências. Como dentro de uma rede uma mesma freqüência é reutilizada varias vezes, é necessário determinar a distancia mínima que deve separar duas células utilizando a mesma freqüência para que nenhum fenômeno perturbador interfira. Calculando a relação entre a potência da portadora e a do ruído, é possível estimar essa distancia.

Praticamente, em um célula um celular recebe tanto a mensagem útil que lhe é destinada, cuja potência chamamos C, quanto um certo número de sinais perturbadores. O conhecimento da relação entre essas potências permitirá conhecer a qualidade da comunicação. Os sinais perturbadores são divididos em duas classes:

1 - As interferências de potências total I, que são devido aos sinais emitidos pelas outras estações. Essas interferências são:

(a) as **interferências co-canal** que são devidas aos sinais emitidos pelas outras estações de base utilizando a mesma freqüência,

(b) as **interferências de canais adjacentes** devidos aos sinais emitidos pelas outras estações de base utilizando freqüências vizinhas.

2 - O ruído, de potência N, vindo principalmente do ruído de fundo do receptor.

Essa relação e dada por : C / (N + I).

2.6 Conceitos de Transmissão

Um (1) site rádio = Estação de Base que pode transmitir até 50 Watts. A potência de transmissão W/cm^2 é limitada por razões de segurança (efeitos sobre o corpo humano).A potência de um terminal móvel é fixada em 2W Max. Quanto mais próximo da estação de base menor a potência de emissão. Para cobrir sua área de atuação o operador é autorizado a utilizar um certo número de freqüência dentro de uma banda especificada (por exemplo, as bandas B1 e B2 dentro da banda de 900MHz, como mostra a Figura 4).

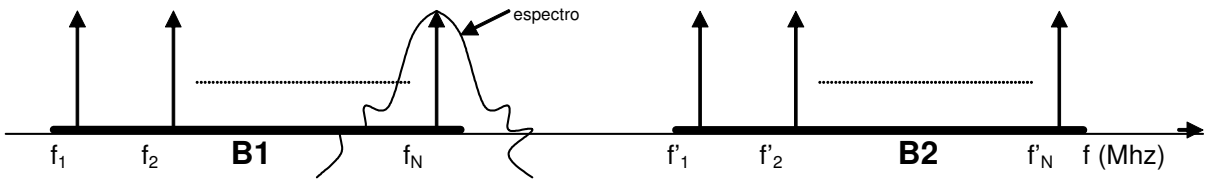


Figura 4 Banda de Freqüência

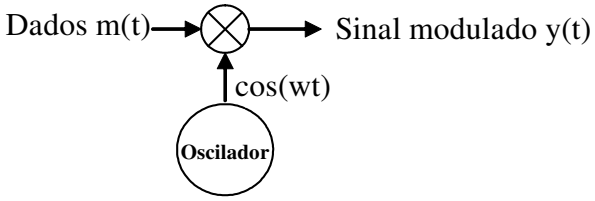


Figura 5 - Exemplo de um sistema de modulação

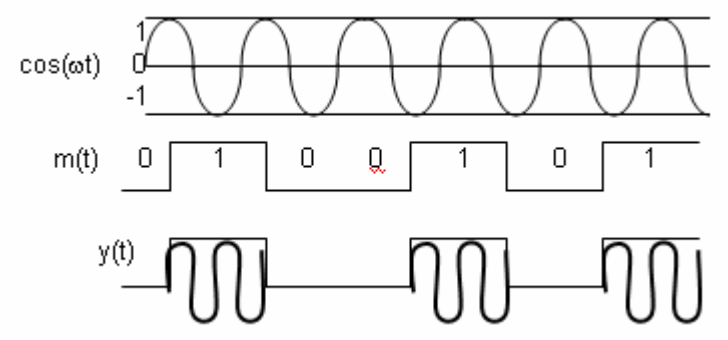


Figura 6 - Sinais envolvidos na modulação

2.6.1 Ocupação do espectro

A Figura 7 mostra várias freqüências portadoras e a ocupação do espectro dessas freqüências e a densidade espectral de potência. A crista do DSP é tomada como referencia de (zero dB).

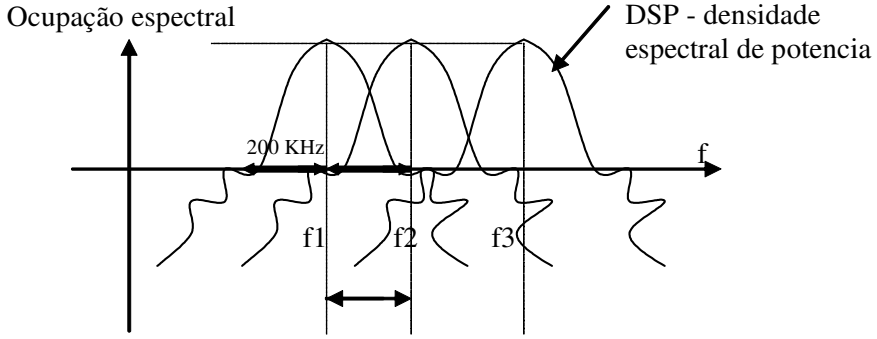


Figura 7 Ocupação do espectro

Notação: 10 $\log_{10}$ (P) = P_{dB} (potência relativa)

Potência relativa de P_1 com relação a P_2 dado por:

$$dB = 10 \log_{10} \frac{P_1}{P_2}$$

Figura 8 Calculo da potência em decibéis

O dBm é utilizado como medida de potência sendo calculado assim:

$$dBm = 10 \log_{10} \left(\frac{P(W)}{10^{-3} W} \right)$$

Figura 9 Calculo da potência em dBm

Por exemplo: 0 dBm ⇒ P = 1 mW e 10 dBm ⇒ P = 10 mW.

O limite da sensibilidade de um celular é de – 110 dBm ⇒ P = $1o^{-11}$ mW

Para o operador o problema a resolver é oferecer o serviço, garantir a qualidade do serviço, assegurar a cobertura rádio. Ele dispõe de N freqüências sobre as quais ele deve transportar as informações. Essas freqüências portadoras representam os recursos a atribuir aos usuários.

2.6.2 Técnicas de utilização de freqüências:

2.6.2.1 FDMA = Frequency Division Multiple Acces

A Figura 10 mostra as freqüências portadoras reservadas para a transmissão no sentido ascendente (UP) e descendente (DOWN). Um par de freqüências **(fi, f'i=fi+D)** é afetado a um celular.

Sentido UP Link: $\mathbf{f_i}$ com $\mathbf{i} \varepsilon [1,n]$ → comunicação celular para BTS.

Sentido Down Link: f_i+**D** → comunicação BTS para celular.

O FDMA é uma técnica analógica simples e confiável, entretanto com má utilização dos recursos. Ela é utilizada nos redes analógicas, tais como:

- AMPS (Advanced Mobile Phone System) nos USA,
- R2000 (450 à 900 Mhz) na Franca,
- NMT (Nordic Mobile Telephony) nos paises escandinavos.

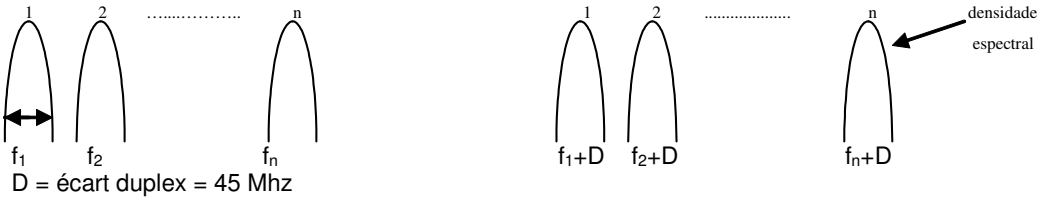


Figura 10 Bandas de freqüência

2.6.2.2 TDMA = Time Division Multiple Access

O método FDMA é melhorado pela combinação com o método TDMA. Neste último método a portadora f_i é atribuída durante 8 intervalos de tempos (IT) a comunicações diferentes. Esses 8 IT, mostrados na Figura 11, constituem uma trama que dura de 5 à 10 ms. Para uma portadora temos 8 comunicações simultâneas no lugar de uma. Se tivermos N portadoras teremos 8N comunicações simultâneas.

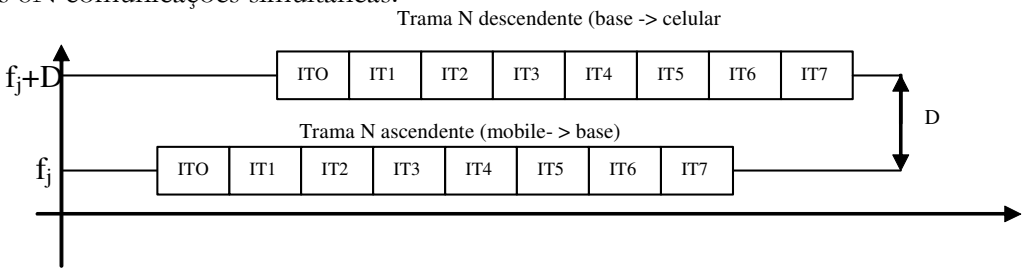
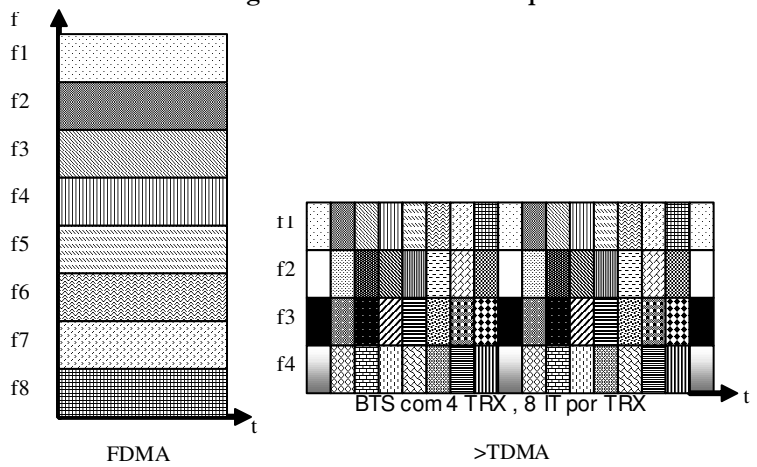


Figura 11 Intervalos de tempo



2.7 PLMN - Rede celular

Um sistema de telefonia celular assegura o "roaming" e o handover sobre um território coberto pela rede. Ele permite a comunicação entre os usuários móveis e os usuários do sistema fixo RTCP (Rede Telefônica Comutada Publica).

Os equipamentos (estação de base, comutadores móveis, etc) são organizados em uma rede chamada PLMN (Public Land Mobile Network). Uma PLMN se compõe de duas partes: um

subsistema rádio e uma de rede de comutação, como mostra a Figura 12. O sistema rádio inclui as estações de base que cobrem o território da PLMN. O sistema de comutação pode ser vista como uma rede telefônica especifica com comutadores adaptados, gateway para a RTCP e de bases de dados locais e centrais de usuários.

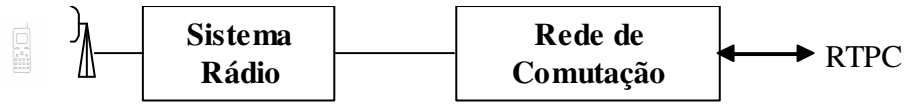


Figura 12 Rede Celular

Unidade 3 Redes Celulares GSM

GSM – Global Móbile System

3.1 Histórico do GSM

A historia da telefonia móvel digital GSM começou realmente em 1982. Nesta data, o Groupe Spécial Mobile, chamado GSM, foi criado pela "Conférence Européenne des administrations des Postes et Télécommuncations" (CEPT) a fim de elaborar as normas de comunicações móveis para a Europa na banda de freqüência de 890 a 915 MHz para a emissão a partir das estações móveis e de 935 a 960 MHZ para a emissão a partir de das estações fixas.

Os anos 80 viram o desenvolvimento do digital tanto ao nível da transmissão quanto ao nível do tratamento do sinal. Assim, em 1987, o grupo GSM fixou as escolhas tecnológicas para uso das telecomunicações móveis: transmissão digital, multiplexagem temporal dos canais rádio, codificação das informações assim como uma nova codificação para a voz. A primeira comunicação experimental do GSM se deu em 1991, na França. A sigla GSM passou a significar "Global System for Mobile communications" e as especificações foram adotadas para os sistemas funcionando na banda de 1800 MHz.

Hoje, as redes GSM estão instaladas no mundo todo e o número de usuários cresce mais e mais.

3.2 Características do GSM

Serviços – O GSM permite a execução dos serviços de voz, dados, fax, correio, etc.

Chip SIM – A utilização de um chip chamado cartão SIM torna a subscrição do usuário independente do terminal móvel.

Interface aérea – Transmissão digital, compartilhamento de tempo, codificação da voz a 13kbits/s. GSM é um sistema TDMA com banda de 200Kbits/s permitindo até oito (8) comunicações simultâneas multiplexada na mesma freqüência.

Dois sistemas são disponíveis:

GSM (Global System Móbile): banda de freqüência de 900MHz

DCS (Digital Cellular System): banda de freqüência de 1800MHz

A Tabela 1 abaixo mostra as principais características dos sistemas GSM e DCS.

Característica	GSM	DCS
Banda de freqüência up	890-915	1710-1785
Banda de freqüência down	935-960	1805-1880
Número de IT por trama TDMA	8	8
Técnica de multiplexagem	Freqüência e tempo	Freqüência e tempo
Diferença Uplink-Downlink	45 MHz	95 MHz
Taxa total de modulação	271 Kbits/s	271 Kbits/s
Taxa de voz	13 Kbits/s	13 Kbits/s
Taxa máxima de dados	12 Kbits/s	12 Kbits/s
Raio das células	0.3 a 30 Km	0.1 a 4 Km
Potência dos terminais	2 a 8 W	0.25 e 1 W
Sensibilidade dos terminais	-102 dB	
Sensibilidade a BTS	-104 dB	

Tabela 1 Características do GSM

3.2.1 Identificação do usuário

Nas redes celulares de primeira geração o número de chamada de um usuário era memorizado dentro do equipamento terminal do usuário e fisicamente ligado a esse terminal. No GSM os terminais não possuem nenhuma configuração e são inutilizáveis como tais. É necessário acrescentar ao terminal um chip chamado SIM (Subscriber Identity Module) que possui na sua memória as características da linha, todas as informações do ambiente do usuário (agenda, senha pessoal, últimos números chamados, etc) e as informações sobre a interface rádio (característica da ultima rede a qual o usuário se conectou). Se um usuário trocar de telefone sem trocar de cartão SIM, a operação é totalmente transparente para a rede. A Figura 13 mostra o terminal móvel e seu chip SIM.

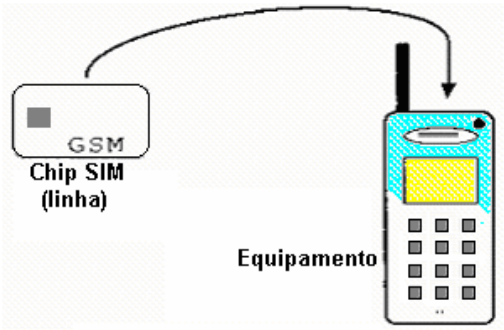


Figura 13 - Chip SIM

Na rede GSM existem uma diferença entre o número e a identificação de um usuário. A identificação é chamada IMSI (International Móbile Subscriber Identity) e permite a rede identificar um usuário de forma única. Ela não é conhecida do usuário, pois esse conhece somente o número chamado MSISDN (Móbile Station Integrated Services Digital Number) através do qual ele pode ser chamado pelos outros usuários. Uma base de dados dentro da rede faz a correspondência entre o número utilizado pelos usuários e o número realmente utilizado dentro da PLMN para localizar o usuário. A utilização do IMSI é ilustrado na Figura 14.

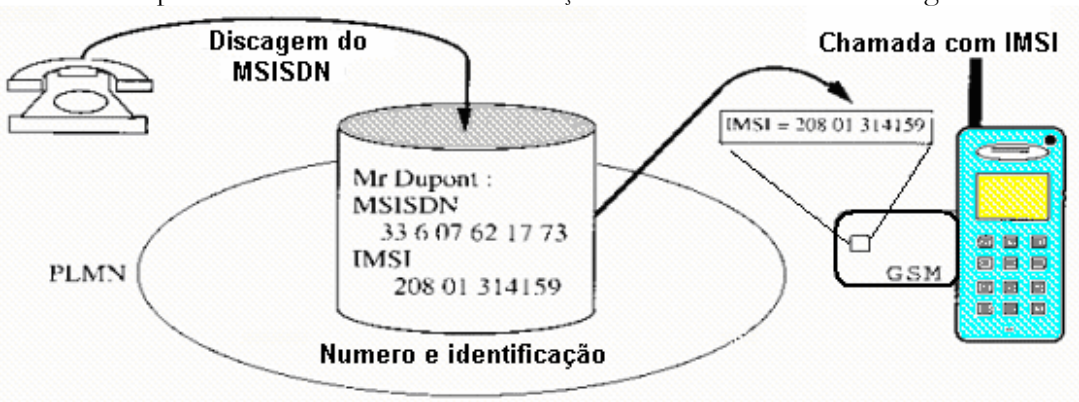


Figura 14 - Utilização do IMSI

Cada equipamento terminal móvel no GSM é identificado pelo IMEI (International Móbile Equipament Identity). A composição desta identificação inclui uma parte que caracteriza o construtor do equipamento. Essa identificação permite detectar e interditar a utilização de equipamentos roubados ou não homologados na rede.

3.2.2 Classificação dos serviços

Os serviços ofertados por uma rede móvel são classificados da seguinte maneira:

1 – Serviços suporte – os serviços suporte ou "bearer services" compreendem a oferta de uma capacidade de transmissão entre duas interfaces de usuários definidas;

2 – Tele-serviços – os tele-serviços compreendem a oferta de uma comunicação que incluem os terminais móveis e as aplicações;

3 – Serviços complementares - reagrupam as facilidades de utilização que podem ser ofertadas em complemento dos serviços suporte e tele-serviços.

Figura 15 Classificação dos serviços

3.2.3 Serviços suporte

A oferta dos serviços suporte consiste a fornecer uma capacidade de transmissão com características técnicas de taxa de transmissão, taxa de erros, modo de transmissão (síncrono/assíncrono). A oferta de uma ligação ponto a ponto digital é um exemplo de um serviço suporte. Os serviços ofertados na rede GSM são relacionados na Tabela 2 abaixo. As taxas de transmissão de dados podem variar entre 300 bit/s a 9.6Kbits/s e podem ser totalmente digitais ou sofrer conversão analógica/digital. Dois modos são possíveis: transparente e não transparente. No modo transparente os dados são transmitidos de forma bruta entre as duas interfaces. No modo não transparente um protocolo, Rádio Link Protocol, assegura a confiabilidade dos dados.

Tipo de Serviço	Taxas (bits/s)	Tipo de acesso	Modo	Comentário
Circuitos de Dados	300, 1200, 2400, 4800 e 9600	Assíncrono	T ou NT	V21, V22 V26 e V32
	1200, 2400, 4800 e 9600	Síncrono	T ou NT	V22, V26 e V32
	BS→ MS 1200 MS→ BS 75	Assíncrono	T ou NT	Chamada via celular
Acesso assíncrono a uma rede de dados	300, 1200, 2400, 4800 e 9600	Assíncrono	T ou NT	
	BS→ MS 1200 MS→ BS 75	Assíncrono	T ou NT	Chamada via celular
Acesso síncrono a uma rede de dados	2400, 4800 e 9600	Síncrono	NT	Chamada via celular

Tabela 2 - Serviços GSM (T – Modo transparente, NT – Modo não transparente)

3.2.4 Tele-serviços

Os principais tele-serviços no GSM são a telefonia, a transmissão de mensagens curtas ou SMS e a transmissão de fax, como mostrados na Tabela 3:

Classe	Denominação	Norma
Transmissão de Voz	Telefonia	Telephony
	Chamada de urgência	Emergency Call
Mensagens Curtas	Mensagem Curta para um celular ponto a ponto	Short Message Mobile Terminating/Point to Point
	Mensagem Curta originada por um celular ponto a ponto	Short Message Mobile Origination/Point to Point
	Mensagem Curta em difusão para os celulares	Short Message Cell Broadcast
Fax	Transmissão alternada voz/fax grupo 3	Alternate speech and facsimile group 3

Tabela 3 Tele-serviços GSM

1 – Telefonia - Consiste na transmissão de voz para poder efetuar comunicações telefônicas. A voz é transmitida no formato digital dentro da rede GSM e depois convertida em analógica.

2 – Mensagens curtas – Esse serviços permite realizar um correio ponto a ponto, bidirecional com confirmação. Esse serviço necessita um servidor de mensagens curtas, Short Message Service Center, que age como intermediário entre os terminais, capaz se estocar e de retransmitir as mensagens. Os SMS podem ser utilizados pelo operador para gerenciar certos serviços, tais como, transmissão de alertas, de tarifação, etc.

3.2.5 Serviços suplementares

Oferece certas melhorias aos serviços suporte e tele-serviços. São exemplos de serviços suplementares: a identificação do número, re-envio de chamada, dupla chamada, conferencia, grupo fechado de usuários, faturamento, restrições de chamada. Os serviços suplementares são resumido na Tabela 4.

Serviço	Denominação	Norma	Abreviação
Identificação do número	Apresentação da identificação da linha chamadora	Calling Line Identification Presentation	CLIP
	Restrição da identificação da linha chamadora	Calling Line Identification Restriction	CLIR
	Apresentação da identificação da linha conectada	Connected Line Identification Presentation	CoLP
	Restrição da identificação da linha conectada	Connected Line Identification Restriction	CoLR
Reenvio de Chamada	Reenvio de chamada Incondicional	Call Forwarding Unconditional	CFU
	Reenvio de chamada por Ocupação	Call Forwarding on Subscriber Busy	CFB
	Reenvio de chamada por "não responde"	Call Forwarding on Subscriber No Reply	CFNRy
	Reenvio de chamada por "não acessível"	Call Forwarding on Subscriber Not Reachable	CFNRc
Dupla Chamada	Colocação em espera	Call Waiting	CW
	Chamada em espera	Call Hold	HOLD
Conferência	Chamada conferencia	Multy-Party Service	MPTY
	Grupo fechado de usuários	Closed User Group	CUG
Faturamento	Indicação de totais	Advice of Charge (Information)	AoCi
	Indicação de totais com Interdição	Advice of Charge (Charging)	AoCC
Restrição de chamadas	Interdição de todas as chamadas de saída	Barring of All Outgoing Calls	BAOC
	Interdição de chamadas internacionais	Barring of Outgoing International Calls	BOIC
	Interdição de todas as chamadas de entrada	Barring of All Incoming Calls	BAIC

Tabela 4 Serviços suplementares

Unidade 4 Arquitetura das Redes GSM

Uma rede GSM se compõe de três subsistemas:

1 - Subsistema rádio – BSS (Base Station Sut-system): assegura as transmissões radioelétricas e controla os recursos rádio;

2 - Subsistema rede – NSS (Network Sub-System): compreende o conjunto de funções necessárias ao estabelecimento das chamadas e a mobilidade;

3 - Subsistema de operação e manutenção - OSS (Operation Susb-System): permite a administração do sistema.

A Figura 16 abaixo apresenta as principais entidades e interfaces dos sistemas BSS e NSS da rede GSM.

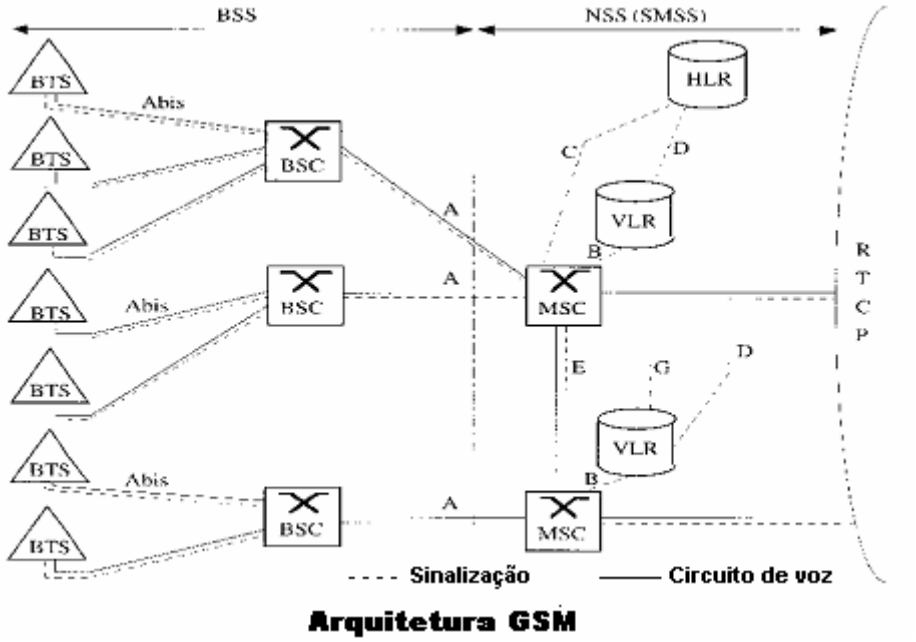


Figura 16 - Arquitetura do sistema GSM

4.1 Base Station System

O BSS compreende:

- BTS (Base Transceiver Station) que são os emissores/receptores de rádio
- BSC (Base Station Controller) que controlam um conjunto de BTS e permitem uma primeira concentração de circuitos.

4.1.1 BTS - Base Transceiver Station

A BTS é um equipamento físico utilizado para realizar a cobertura rádio que determina uma zona geográfica chamada "célula". Uma BTS compreende:

- Um local técnico que abriga as placas de circuito radioelétricas e seu sistema de alimentação de energia.
- Um sistema de antenas de emissão / recepção
- Cabos coaxiais que ligam as placas eletrônicas as antenas.

Uma célula pode ter uma BTS do tipo omni-direcional ou várias BTS do tipo setorial, como mostra a Figura 17.

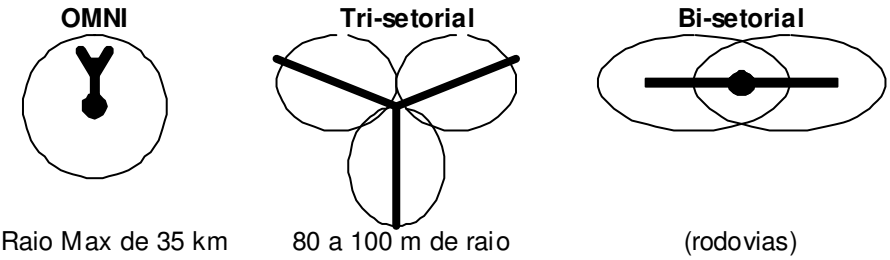


Figura 17 – Tipos de antenas de BTS

4.1.2 Funções da BTS

- A BTS é um conjunto de emissores/receptores chamados TRX. Ela é responsável pelas transmissões rádio/ modulação, demodulação, equalização, codificação corretora de erros, etc.
- Ela gerencia toda a camada física: multiplexação TDMA, salto de freqüência, criptagem. Ela realiza as medidas radioelétricas necessárias a verificação que uma comunicação em curso transcorre corretamente (controle de potência por exemplo).
- Ela gerencia a camada Data Link para a troca de sinalização entre o celular a infra-estrutura bem como para assegurar a confiabilidade dos diálogos.

4.1.3 Capacidade de uma BTS

A capacidade de escoamento de trafego é medido em Erlang.

$$\text{Erlang: } \frac{\textit{Tempo de ocupaçao do circuito}}{\textit{Tempo de observaçao do circuito}}$$

A capacidade teórica máxima de uma BTS é de 16 TRX. Entretanto, na prática os valores de tráfegos medidos são mostrados na Tabela 5.

1 TRX : 2,3 Erlangs	5 TRX : 27 Erlangs
2 TRX : 8,2 Erlangs	6 TRX : 35 Erlangs
3 TRX : 14,1 Erlangs	7 TRX : 42 Erlangs
4 TRX : 20,6 Erlangs	8 TRX : 49 Erlangs

Tabela 5 - Capacidade da BTS

4.1.4 Potência de uma BTS

A norma GSM distingue as BTS normais das micro-BTS. As BTS normais são aquelas estações de base, clássicas, com equipamentos instalados em locais técnicos e as antenas sobre os telhados interligados por cabos. A norma prevê as potências resumidas na Tabela 6 para essas estações.

	GSM 900		DCS 1800	
Número da Classe	Potência Máxima (W)	Limite Maximo de Potência	Potência Máxima (W)	Limite Maximo de Potência
1	320	640	20	40
2	160	320	10	20
3	80	160	5	10
4	40	80	2.5	5
5	20	40		
6	10	20		
7	5	10		
8	2.5	5		

Tabela 6 - Classes de potência das BTS normais

As micro-BTS são previstas para assegurar a cobertura das zonas urbanas densas que são divididas em micro-células. Esses equipamentos são de pequenos tamanhos sendo mais numerosos que as BTS normais. A norma propõe potências pequenas para limitar o alcance e permitir o funcionamento duas BTS próximas. A Tabela 7 abaixo mostra as classes de potência das BTS enquanto a Tabela 8 mostra a sensibilidades das BTS.

	GSM 900		DCS 1800	
Classe	Potência Máxima (W)	Limite Maximo de Potência	Potência Máxima (W)	Limite Maximo de Potência
M1	0.08	0.25	0.5	1.6
M2	0.03	0.08	0.16	0.5
M3	0.01	0.03	0.05	0.16

Tabela 7 - Classes de Potência das micro-BTS

Tipo de BTS	GSM 900	DCS 1800
Micro M1	-97 dBm	-102 dBm
Micro M2	-92 dBm	-97 dBm
Micro M3	-87 dBm	-92 dBm
BTS normal	-104 dBm	-104 dBm

Tabela 8 - Sensibilidade das BTS

4.1.5 Configuração das BTS

Existem diferentes configurações BTS-BSC, entretanto as mais comuns são as configurações estrela ou barra, como mostra a Figura 18 abaixo:

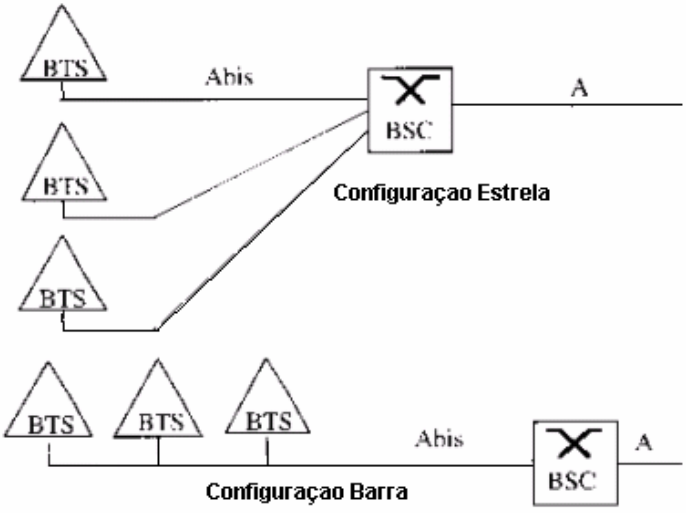


Figura 18 Configuração das BTS

4.1.6 BSC - Base Station Controller

É o órgão inteligente do BSS. Sua função principal é controlar os recursos rádio. Ele comanda a alocação dos canais, utiliza as medidas efetuadas pelas BTS para controlar a potência de emissão do celular e da BTS e toma as decisões de handover. É um comutador que concentra os circuitos que vão para a rede.

Os construtores utilizaram diferentes filosofias na concepção dos BSC. Alguns conceberam BSC de pequenas capacidades visando multiplicar sua quantidade na rede e diminuir a distancia BTS-BSC. É uma filosofia mais adaptada às redes rurais. Outros conceberam BSC de grande capacidade para serem utilizadas em redes urbanas de grande densidade de tráfegos. A capacidade de um BSC está compreendida entre 100 e 900Erlang.

Funções Principais:

- alocação de canais rádio para os terminais,
- gerência do salto de freqüência,
- tratamento das medidas rádio recebidas da BTS e dos terminais,
- transferência intercelular (handover),
- controle da sinalização.

BSC analisa as seguintes medidas para decidir o handover:

- Uplink: - terminal mede o nível de potência recebida (RX Level) das BTS (6 possíveis) durante 4 IT diferentes dos que ele utiliza,
  - o terminal mede a qualidade da comunicação (RX Quality).
- Downlink: - a BTS mede o RX Level, RX Quality, e a distancia **d** do terminal.

4.2 Subsistema Rede

O NSS compreende:

- MSC (Móbile-service Switching Center) que são os comutadores celulares associados às bases de dados VLR (Visitor Location Register)
- HLR (Home Location Register) que é uma base de dados de localização e de característica dos usuários.

4.2.1 HLR – Home Localization Register

O HLR é uma base de dados que gerencia os usuários de uma dada PLMN. Ele armazena as informações dos usuários tais como:

- a identificação internacional de usuário (IMSI) utilizado na rede;
- o número de chamada do usuário (MSISDN);
- o perfil do usuário (serviços suplementares autorizados, autorização de chamadas internacional, etc).
- Tipo e número de re-encaminhamento de chamadas.

Esses dados são armazenados pelo operador a partir do sistema de administração. O HLR armazena também as informações de localização dos usuários, que são enviadas pelos celulares através da rede.

O HLR pode ser centralizado ou distribuído. No primeiro caso uma grande máquina gerencia varias centenas de milhares de usuários. No segundo caso ele pode ser integrado no MSC e para armazenar os dados dos usuários que se comunicam preferencialmente com esses MSC. Em todo caso, um usuário é associado a um único HLR de forma independente de sua localização. A rede identifica o HLR a partir do número MSISDN ou do IMSI.

4.2.2 MSC/VLR – Móbile Switching Center/Visitor Localization Register

O MSC é o centro de comutação celular. Suas funções principais são:

- Assegurar o interfuncionamento da rede GSM com as outras redes de telecomunicações.
- Executa funções de comutação para os terminais visitantes dentro das células da zona de cobertura da rede.
- É o ponto de passagem obrigatório de toda comunicação.
- Controlar o estabelecimento das comunicações entre um celular e um outro MSC, a transmissão de SMS e a execução de handover (do qual ele deve participar).
- Dialogar com o VLR para gerenciar a mobilidade dos usuários.
- Ele pode funcionar como GMSC (Gateway MSC) que é ativado no inicio de cada chamada de um telefone fixo para um móvel.

O VLR é o responsável pelo registro da localização LA (Location Área) dos usuários visitantes. É uma base de dados que memoriza os dados dos usuários que estão presentes na zona

geográfica controlada por um MSC. Os dados armazenados no VLR são similares aos dados do HLR, acrescentados da identidade temporária TMSI.

A maioria dos construtores integra o VLR dentro do MSC, simplificando o dialogo entre as duas entidades da rede. Um conjunto MSC/VLR pode gerenciar uma centena de milhares de usuários para um tráfego médio de 0.025Erlang por usuário.

4.3 Subsistema de operação e manutenção

4.3.1 Administração da rede

A administração da rede (Network Management) compreende todas as atividades que permitem armazenar e controlar a performance e a utilização dos recursos de forma a oferecer um certo nível de qualidade aos usuários.

As diferentes funções da administração são:

- A administração comercial (usuários, terminais, faturamento, estatística, etc),
- A gerência da segurança (detecção de intrusos, etc),
- A gerência da performance (observação do trafego e da qualidade, etc),
- Controle da configuração do sistema (novos equipamento, atualização de softwares, etc),
- Manutenção (detecção de falhas, testes de equipamentos, etc).

O sistema de administração da rede GSM se baseia no conceito TMN (Telecommunications Management Network).

4.3.2 Arquitetura do TMN

A administração das primeiras redes se fazia individualmente em cada equipamento a partir de um terminal diretamente conectado a eles. Entretanto, a complexidade atual das redes necessita de ferramentas de administração que representem seu estado e sua configuração de forma mais adequada, tais como representação gráfica dos equipamentos, histogramas de carga, etc. O conjunto das funções necessárias é o Sistema Operacional. Esse nível de administração global deve ser independente dos equipamentos. É necessário então integrar equipamentos de mediação entre os equipamentos da rede (BTS, BSC, etc) e o sistema operacional. O conjunto formado pelos equipamentos de mediação, o sistema operacional e a redes de transporte utilizadas formam a rede de operação e manutenção das telecomunicações ou TMN, como mostrado na Figura 19.

4.3.3 EIR – Equipment Identity Register

É uma base de dados que contem todos as identidades ou IMEI dos terminais da rede. Ele pode ser consultado por serviços que verificam se um determinado terminais é autorizado a funcionar na rede ou não.

O EIR contém uma "lista branca" dos terminais autorizado, uma "lista negra" contendo a identificação dos equipamentos roubados ou de acesso interditado na rede e uma "lista cinza" dos equipamentos que apresentam algum tipo de irregularidade, mas insuficientes para justificar uma interdição total de acesso à rede.

4.3.4 AUC – AUtentication Center

O centro de autenticação armazena para cada usuário uma senha secreta utilizada para autenticar as solicitações de serviços e para "criptar" as comunicações. Um AUC é associado a um HLR, entretanto eles não fazem parte do mesmo subsistema.

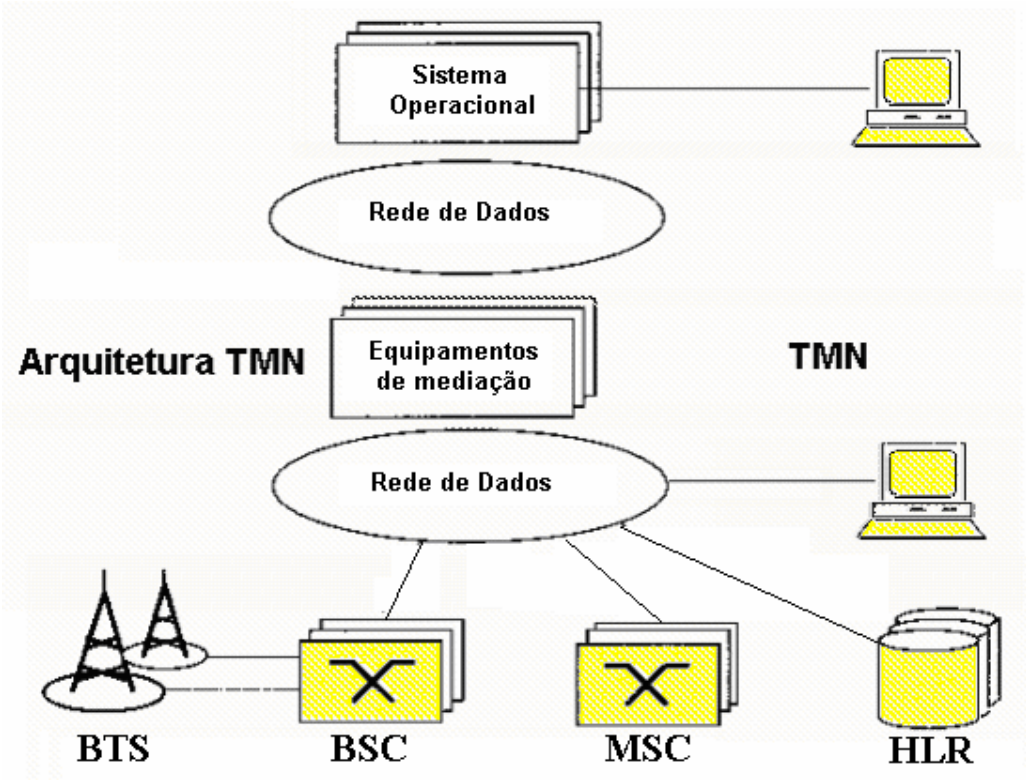


Figura 19 – Arquitetura da rede TMN GSM

4.4 As Interfaces GSM

As interfaces interligam as entidades da rede GSM. Cada interface, designada por uma letra, é especificada pela norma GSM. A Tabela 9 abaixo mostra a nomenclatura das interfaces GSM:

Nome	Localização	Utilização
Um	MS—BTS	Interface Rádio
Abis	BTS—BSC	Diversos
A	BSC—MSC	Diversos
C	GMSC—HLR	Interrogação do HLR para chamada de entrada
	SM-GMSC—HLR	Interrogação do HLR para SMS de entrada
D	VLR—HLR	Gestão de informações de usuários e de localização
	VLR—HLR	Serviços suplementares
E	MSC—SM-GMSC	Transporte de mensagens curtas (SMS)
	MSC—MSC	Execução de handover
G	VLR—VLR	Gestão de informações de usuários
F	MSC—EIR	Verificação da identificação do terminal móvel
B	MSC—VLR	Diversos
H	HLR—AUC	Troca de dados de autenticação

Tabela 9 - Lista das interfaces GSM

A interface D deve ser rigorosamente respeitada por todos os fabricante e operadores, pois ela permite a um MSC/VLR de uma rede dialogar com o HLR de todos as outras redes existentes. Sua conformidade com a norma permite o roaming nacional e internacional.

A interface A separa o NSS do BSS. A conformidade com a norma permite aos operadores ter diferentes fabricantes para o NSS e para o BSS.

4.5 As camadas de Protocolo

A norma GSM estrutura os protocolos usados na rede em camadas seguindo a filosofia de camadas OSI. Essas camadas de protocolo são mostradas na Figura 20 abaixo:

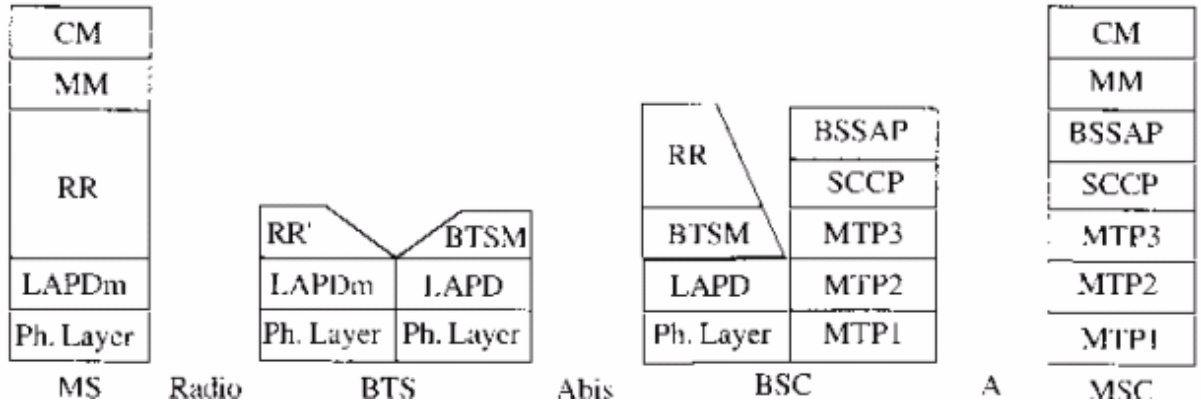


Figura 20 Protocolos GSM

4.5.1 Camadas de protocolo na BSS

No BSS existem 3 camadas de protocolos:

- a camada física,
- a camada de enlace,
- a camada de rede.

A camada física (camada 1) define o conjunto de meios de transmissão e recepção física da informação. Na interface Abis a transmissão é digital a 64kbis/s. A camada 2 (enlace) tem por objetivo tornar confiável a transmissão entre dois equipamentos por um protocolo que implementa mecanismos de confirmação e de retransmissão. A interligação entre a BTS e o BSC é controlado pelo protocolo LAPD e a interligação entre a MS e a BTS é controlada pelo protocolo LAPDm (m de móbile).

A camada 3 tem o objetivo de estabelecer, manter e liberar os circuitos comutados com um usuário da rede fixa. Essa camada é subdividida em 3 subcamadas.

Os tratamentos relacionados com o aspecto puramente rádio são integrados na subcamada RR (Rádio Resource). A camada RR controla o estabelecimento, a manutenção e a liberação dos diferentes canais lógicos TDMA. Na MS a camada RR seleciona as células e utilizando-se das medidas efetuadas pela camada física. A camada 3 está presente principalmente na MS e no BSC. Entretanto algumas mensagens desse protocolo envolvem diretamente a BTS. Na BTS os protocolo da camada 3 são:

- RR' (Rádio Resource Linha) para comunicação com as MS e
- BTSM (BTS Management) para comunicação com o BSC.

O protocolo MM (Mobility Management) gerencia o roaming (localização e autenticação). A subcamada CM (Conection Management) controla as conexões entre a MS e o MSC, sendo composta de 3 partes:

- CC (Call Control) controla as conexões de circuitos com o usuário final,
- SMS (Short Message Service) assegura a transmissão e recepção dos SMS e
- SS (Suplementary Service) controla os serviços suplementares.

Os protocolos CM e MM não são tratados dentro do BSS.

A interface A entre o NSS e o BSS é baseada no SS7 (Signalling Sémaphore número 7) utilizando-se os protocolo MTP (Message Transfert Part) e SCCP (Signalling Connection Control Part) em modo conectado. O protocolo BSSAP (BSS Aplication Part) é responsável pelas mensagens de gerencia entre o BSC e o MSC tornando o BSC transparente as mensagens trocadas entre a MS e o MSC.

4.6 O terminal móvel

O terminal móvel é o equipamento terminal munido do cartão SIM que permite acessar a rede. São divididos em classes de acordo com a potência de emissão, como mostra a Tabela 10. A maior parte dos terminais GSM 900 vendidos são de classe 4 com potência de 2W enquanto que os DCS 1800 são de potência de 1W.

Os terminais reduzem a potência de emissão seguindo os comando da rede. O nível de emissão mínimo no GSM é de 3mW (5 dBm) e no DCS é de 1 mW (0 dBm). A sensibilidade mínima dos terminais é de -100 dBm e -104dBm para os terminais DCS e GSM respectivamente.

	GSM		DCS 1800	
Número da Classe	Potência máxima (W)	Intervalo Admissível (W)	Potência máxima (W)	Intervalo Admissível (W)
1	-	-	1	0.63 : 1.6
2	8	5.0 : 12.7	0.25	0.16 : 0.4
3	5	3.2 : 7.9	4	2.5 : 6.3
4	2	1.3 : 3.2	-	-
5	0.8	0.5 : 1.3	-	-

Tabela 10 - Classes de potência dos terminais

Emissor-Receptor - A Figura 21 abaixo mostra o diagrama em bloco do sistema de emissão do telefone celular.

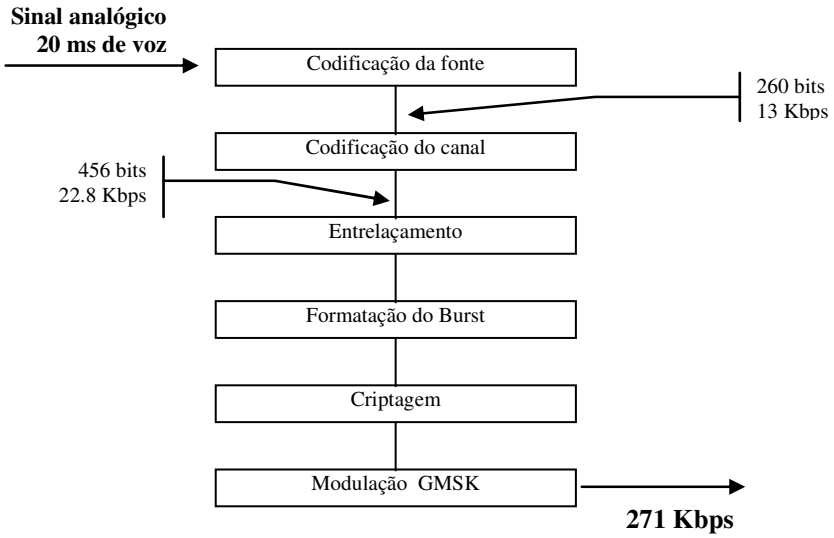


Figura 21 – Sistema de transmissão da voz

Codificação da fonte - O sinal analógico proveniente do microfone do telefone celular é e digitalizado conforme a diagrama da Figura 22 e Figura 23 abaixo:

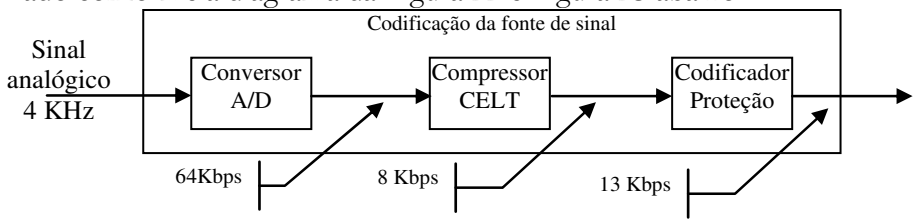


Figura 22 – Sistema de codificação da voz

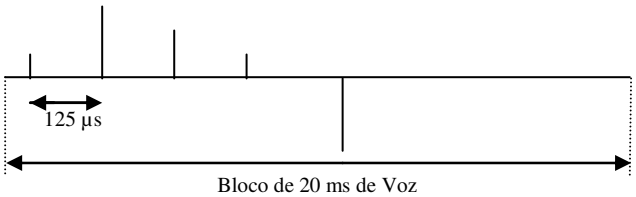


Figura 23 – Amostragem da Voz

Codificação do canal – Acrescenta-se os bits de paridade e de redundância para corrigir os erros devidos a transmissão na interface aérea.

Entrelaçamento - Divide-se os 456 bits de voz em 8 blocos para serem transmitidos em 8 ITs consecutivos. Em caso de problema perde-se somente ¼ dos 456 bits.

Unidade 5 Redes Celulares GSM

5.1 Gerência do Roaming e da Segurança

A introdução da mobilidade nas redes celulares implicou na definição de novas funções com relação às redes fixas. A PLMN deve conhecer a todo o momento a localização dos usuários de forma mais ou menos precisa. Essa função é chamada de roaming. Contrariamente as redes fixas onde o número do terminal corresponde a um endereço físico, o número de um terminal móvel é um endereço lógico constante ao qual é necessário fazer uma correspondência com um endereço físico que varia constantemente devido ao movimento dos usuários. É necessário então que:

1- o sistema conheça em permanência a localização de cada terminal para poder conectá-lo;

2- o terminal fique "ativo", isto é, em estado de alerta de forma a sinalizar seus movimentos ao sistema mesmo na ausência de comunicação.

O roaming gera um tráfego de sinalização na interface aérea e na rede mesmo na ausência de comunicações, enquanto que nas redes fixas um terminal inativo (que não está em comunicação) não gera nenhum tráfego na rede. Por outro lado, a utilização da interface aérea torna as comunicações vulneráveis às escutas e as utilizações fraudulentas. O GSM prevê quatro serviços de segurança, recorrendo aos procedimentos seguintes:

1- autenticação de cada usuário antes de autorizar o acesso a um serviço;

2- utilização de uma identidade temporária;

3- criptagem das comunicações (sinalização e dados dos usuários).

5.2 Numeração e identificação

O sistema GSM utiliza quatro tipos de endereço de usuários:

a) IMSI (International Móbile Subscriber Identity) – identificação invariável de um usuário que é conhecida somente no interior da rede, devendo ficar secreta tanto quanto possível.

b) TMSI (Temporary Móbile Subscriber Identification) – é uma identificação temporária utilizada para identificar o usuário durante as interações entre as MS e a rede.

c) MSISDN (Mobile Station ISDN Number)

d) IMEI (International Mobile Equipment Identify).

5.2.1 IMSI - International Móbile Subscriber Identity

Cada usuário dispõe de uma identificação IMSI única que não varia (exceto no caso de troca do SIM). O IMSI segue o plano de identificação E.212 do IUT. Por questões de segurança (intrusos podem interceptar e utilizar o IMSI fazendo-se passar pelo usuário real) e confidencialidade (intrusos podem escutar o canal rádio e identificar o usuário em comunicação) o IMSI é transmitido na interface aérea em casos raros, tais como quando o TMSI não está disponível. O IMSI, mostrado na Figura 24, é formado dos seguintes partes:

- MCC - Móbile Country Code – indicação do país domicilio do usuário (França=208).
- MNC – Móbile Network Code – indicação da PLMN do usuário (TIM, Oi, etc).
- MSIN – Móbile Subscriber Identification Number – número do usuário dentro da rede GSM.

Os campos MCC e MNC permitem identificar de forma única a PLMN do usuário no mundo todo. Os dois primeiros campos do MSIN (H1H2) identificam o HLR do usuário dentro da PLMN. Isso permite ao MSC identificar o Home do usuário a partir de seu IMSI.

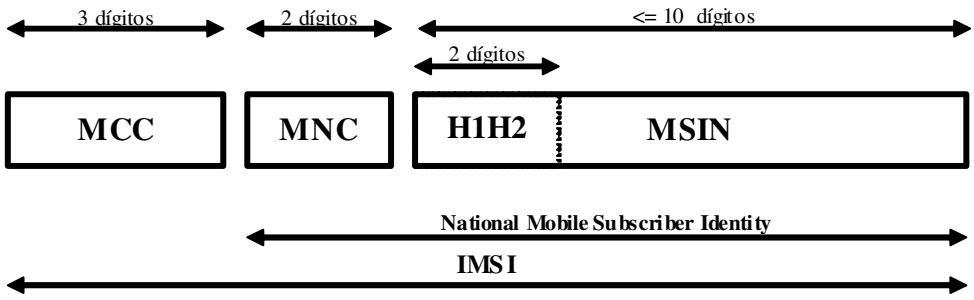


Figura 24 - Formato do IMSI

5.2.2 TMSI - Temporary Móbile Subscriber Identity

É a identificação temporária do usuário dentro da zona controlada/gerenciada por um MSC/VLR. Ela é atribuída de forma local, isto é, unicamente para a zona gerenciada pelo VLR de onde o terminal se encontra. O TMSI é conhecido somente entre a MS e o MSC/VLR. A cada troca de VLR um novo TMSI é atribuído ao usuário.

A utilização do TMSI é opcional, podendo o operador optar pela utilização somente do IMSI (negligenciando a segurança e a confidencialidade). Por isso a estrutura do TMSI (codificado por 4 bytes) é livre.

5.2.3 MSISDN - Mobile Station ISDN Number

É o número do usuário GSM utilizado para as comunicações com as outras redes. Só o HLR contem a tabela de correspondência entre o MSISDN e o IMSI de um usuário.

O MSISDN, mostrado na Figura 25, é conforme a numeração telefônica internacional E.164, sendo composto de 3 campos:

- CC – Country Code - é o código que identifica o pais do usuário (França 33, Brasil 55).
- NSDC – National Significant Móbile Number - o número nacional do usuário é composto dos seguintes campos:
- NDC – National Destination Code – identifica a PLMN do usuário dentro do pais.
- SN – Subscriber Number – Identifica o usuário dentro da rede, sendo atribuída livremente pelo operador da rede.

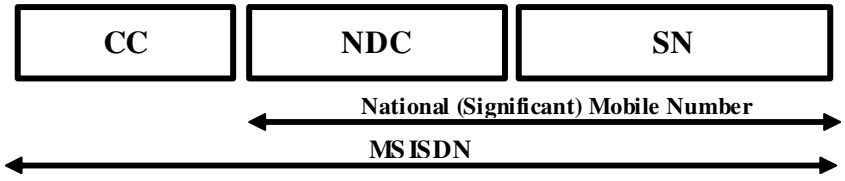


Figura 25 - Formato do MSISDN

Os primeiros dígitos do número SN permitem conhecer o HLR do usuário.

Os campos CC e NDC permitem o roteamento de mensagens entre uma PLMN qualquer e o HLR do usuário.

O exemplo da França: MSISDN tem o formato 33 6 AB PQ MCDU, onde:

- 6 → digito indicativo da rede móvel GSM
- AB → identifica a PLMN
- PQ → identifica o HLR dentro da rede
- MCDU → usuário.

5.2.4 MSRN - Mobile Station Roaming Number

Tem por função permitir o roteamento das chamadas entrantes diretamente do comutador gateway GMSC para o comutador do terminal móvel MSC. Ele é atribuído pelo VLR corrente do terminal móvel de forma temporária e única logo que se estabelece uma chamada com destino ao terminal móvel. Ele tem a mesma estrutura do MSISDN.

A Figura 26 mostra como exemplo da utilização do MSRN uma chamada entrante:

1 – o MSISDN é digitado pelo chamador. A chamada é roteada pela rede fixa até o GMSC mais perto.

2 – O GMSC interroga o HLR para saber para qual MSC ele deve re-encaminhar a chamada.

3 – O HLR traduz o MSISDN em IMSI e interroga o VLR do usuário utilizando o IMSI.

4 – O VLR do usuário atribui um MSRN ao usuário e transmite esse número ao HLR.

5 – Ao receber esse número o HLR o transmite ao GMSC.

6 – O GMSC re-encaminha a chamada para o MSC corrente do usuário como se fosse uma chamada telefônica normal para um usuário de número MSRN.

7 – O MSC chama o terminal utilizando o TMSI que lhe atribuído no momento da entrada do terminal na zona.

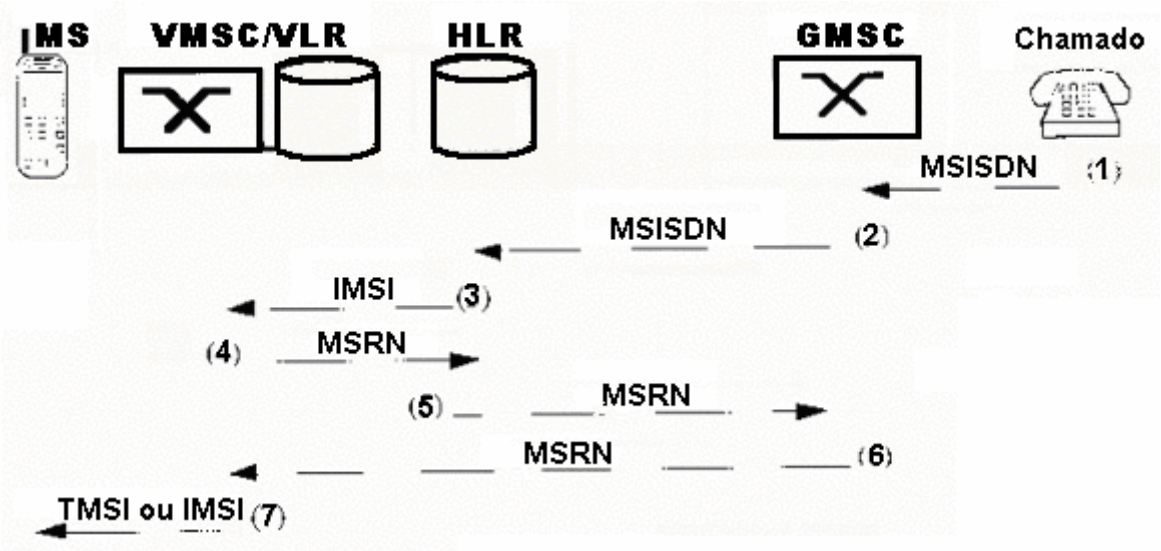


Figura 26 – Utilização do MSRN

5.2.5 IMEI – International Mobile Equipment Identify

O IMEI, mostrado na Figura 27, identifica de maneira única o equipamento móvel sendo codificado da seguinte forma:

- TAC – Type Approval Code – 6 bytes que identificam o construtor do equipamento,
- FAC – Final Assembly Code – 2 bytes que identificam o local de fabricação do equipamento
- SNR – Serial Number – 6 bytes utilizado pelo fabricante,
- Spare – Dígito reservado,

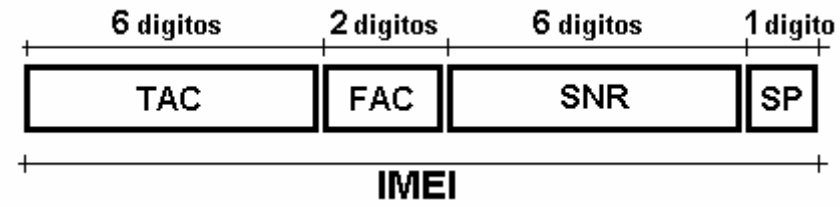


Figura 27 – Formato do IMEI

5.3 Autenticação e criptagem

Para proteger seus usuários e operadores o GSM integra as seguintes funções:

- confidencialidade do IMSI
- autenticação do usuário,
- confidencialidade dos dados do usuário,
- confidencialidade das informações de sinalização.

5.3.1 Confidencialidade do IMSI

Objetiva evitar a interceptação do IMSI durante sua transferência na interface aérea por pessoas, entidade ou processos não autorizados. Isso permite assegurar a confidencialidade da identificação dos usuários e reforçar o nível de segurança da rede.

O melhor meio de evitar a interceptação do IMSI é transmiti-lo o mais raramente possível na interface aérea. Para isso o GSM utiliza o TMSI. Em geral, o IMSI é transmitido somente quando o terminal móvel (celular) é ligado (On/Off). A partir daí a rede utiliza o TMSI para se comunicar com o celular. Somente no caso de perda do TMSI (pane ou perda dessa informação) que a transmissão do IMSI poderá ser necessária.

A Figura 28 abaixo mostra a alocação do TMSI pelo VLR.

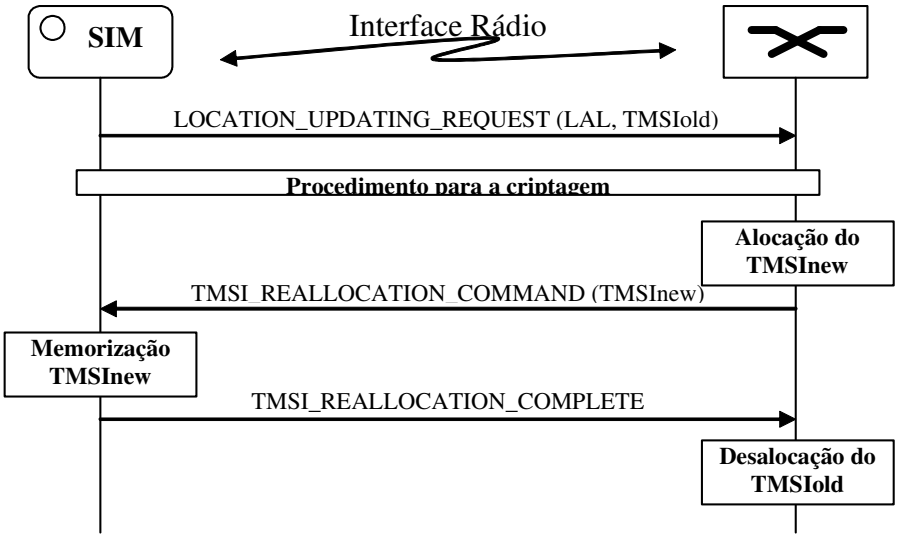


Figura 28 – Alocação do TMSI

5.3.2 Autenticação e criptagem

Para a autenticação e criptagem das informações o GSM utiliza os seguintes elementos:

- um número aleatório RAND (RANDom number),
- uma chave Ki (Identification Key) para autenticação e determinação da chave de criptagem Kc (Ciphering Key),
- um algoritmo A3 (algoritmo de autenticação) que fornece um número SRES (Signed RESult) utilizado para assinatura a partir dos argumentos de entrada RAND e Ki,
- um algoritmo A8 para a determinação da chave Kc a partir dos argumentos RAND e Ki,
- um algoritmo A5 que utiliza a chave Kc para a criptagem dos dados trocados entre a MS e a rede.

A cada usuário é atribuída uma chave Ki associada ao IMSI que se encontra no chip SIM e no AUC. Os algoritmos A3, A5 e A8 são comum a todos os usuários. Os números

RAND, SRES e Kc são agrupados em uma informação tripla. A utilização desses elementos é mostrada na Figura 29 abaixo:

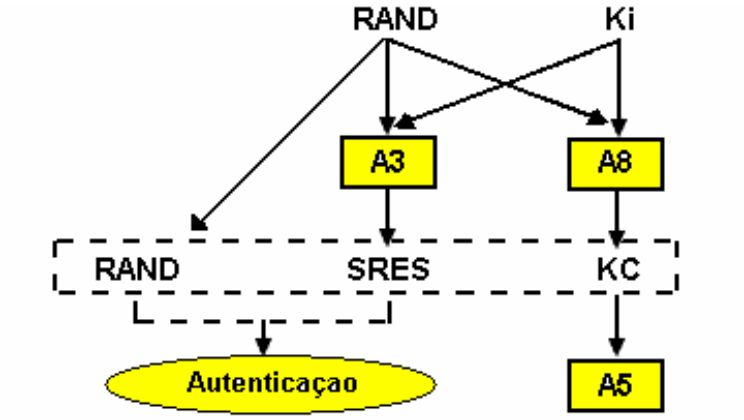


Figura 29 – Autenticação e criptagem

5.3.3 Autenticação do usuário

A autenticação permite verificar que a identificação do usuário na interface aérea (IMSI ou TMSI) é correta a fim de proteger a rede das utilizações fraudulentas de seus recursos e proteger o usuário da utilização de sua conta por outras pessoas. A autenticação pode ser exigida pela rede durante a atualização da localização, o estabelecimento de chamadas e antes de ativar certos serviços suplementares. Se a autenticação do usuário falhar, o acesso à rede é negado.

O procedimento de autenticação, mostrado na Figura 30, se passa da seguinte maneira:

- a rede transmite um número aleatório **RAND** ao celular,
- o chip SIM do celular calcula a assinatura de RAND graças ao algoritmo **A3** e a chave **Ki** (informação secreta). O resultado calculado chamado SRES é enviado a rede.
- a rede compara o SRES recebido ao SRES por ela calculado. Se os dois resultados são iguais o usuário está autenticado.

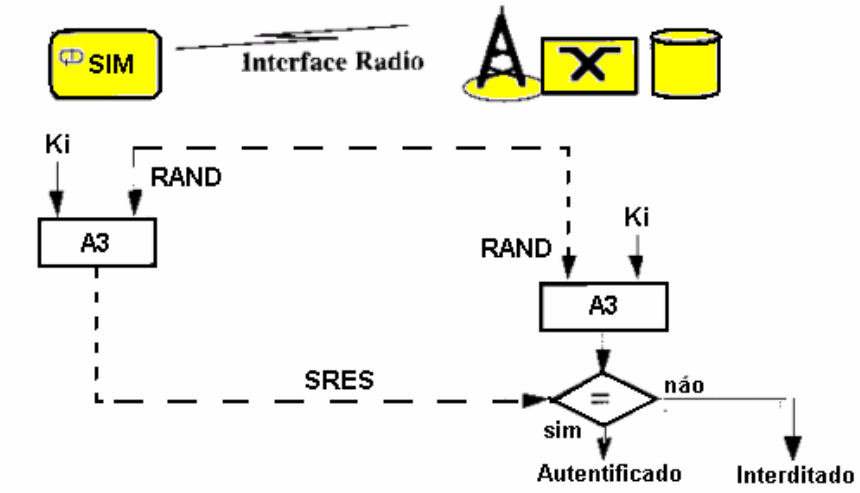


Figura 30 – Autenticação do usuário

5.3.4 Confidencialidade dos Dados

A confidencialidade dos dados evita a interceptação e decodificação das informações do usuário e da sinalização. Ela protege particularmente o IMEI, o IMSI e o número dos usuários chamados. Ela é obtida graças a um processo de criptagem (algoritmo A5) realizada nas informações trocadas entre a MS e a BTS.

A criptagem é baseada na chave **Kc** calculada com os mesmos argumentos da autenticação, mas com um algoritmo diferente, conforme mostra a Figura 31 abaixo:

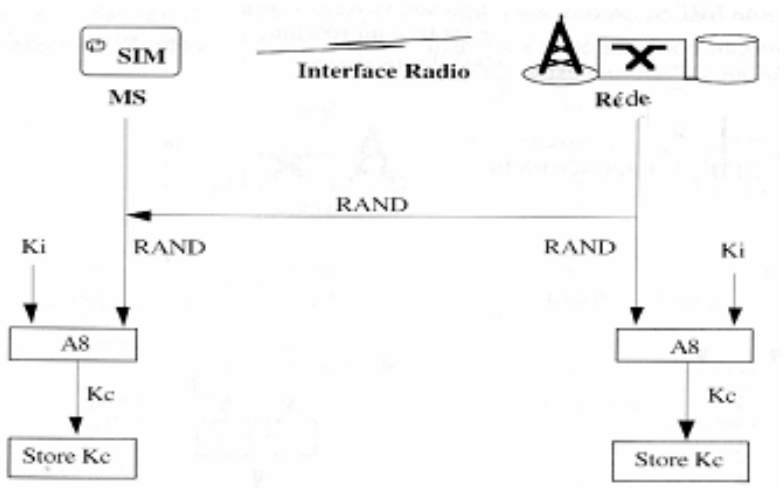


Figura 31 – Geração da chave de criptagem Kc

5.3.5 Gerência dos dados de segurança

A chave Ki é atribuída ao usuário no momento sua inscrição na PLMN juntamente com o IMSI. Ela é armazenada dentro do SIM e dentro do AUC. A fim de limitar as possibilidades de leitura da chave Ki ela não é nunca transmitida através da interface aérea nem entre as entidades da rede de comutação.

A rede não calcula os dados de segurança em tempo real, isto é, no momento que ela precisa. Informações triplas RAND, SRES, Kc são enviadas do HLR para o MSC/VLR através do protocolo chamado MAP. O AUC prepara informações triplas para cada usuário e os transmite ao HLR que os estoca em reserva. Quando o MSC precisa de uma informação tripla, ele envia ao HLR a mensagem MAP_SEND_AUTHENTICATION_INFO contendo o IMSI do usuário. Em resposta o HLR envia 5 informações triplas ao MSC, pois uma informação tripla é destruída logo após sua utilização. Notemos que nenhuma informação confidencial (Ki, A3, A5 e A8) são transmitidos na interface aérea ou na rede de comutação, pois os argumentos necessários RAND e SRES são fornecidos. Seria necessário interceptar milhões de RAND e SRES para determinar o algoritmo A3.

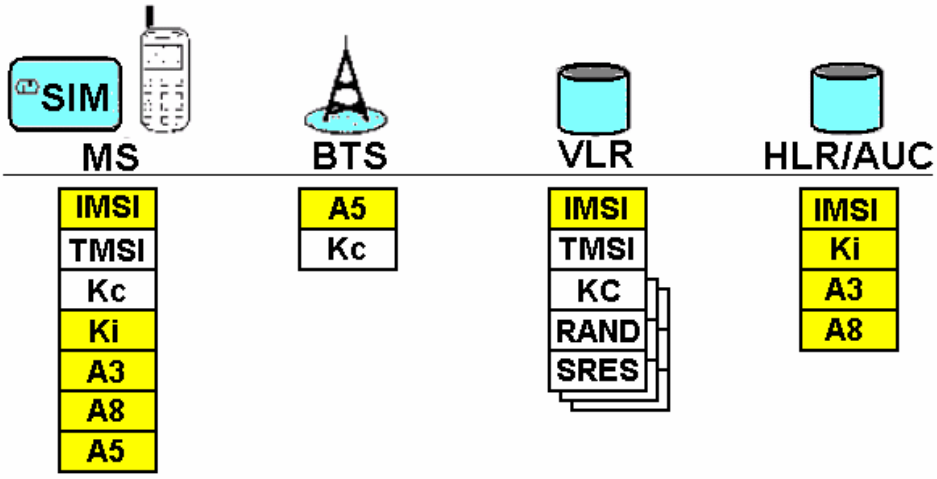


Figura 32 – Dados de segurança nas entidade da rede

Os dados de segurança são armazenados nas entidades da rede (ver Figura 32) da seguinte maneira:

- AUC: algoritmo de autenticação A3, algoritmo de geração de chave de criptagem A8 e as informações IMSI e Ki de cada usuário.
- HLR: várias informações triplas para cada IMSI.
- VLR: várias informações triplas, TMSI (ou IMSI) e chave Kc.
- BTS: algoritmo de criptagem A5 e chave Kc.
- MS: algoritmos A3, A5 e A8, chave Ki, IMSI e TMSI.

A Figura 33 abaixo resume os processos de transferência dos dados de segurança.

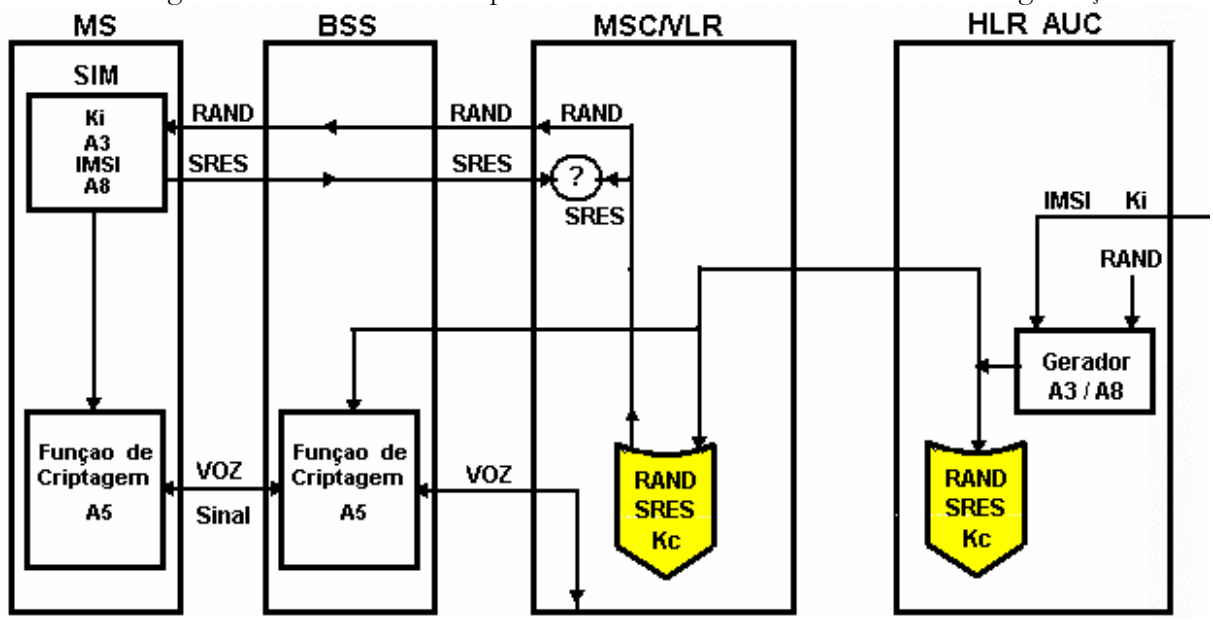


Figura 33 – Processo de transferência dos dados de segurança

5.4 Gerência da localização (roaming)

O principal objetivo da gerencia da localização é permitir ao sistema conhecer a todo o momento a posição de um terminal móvel. Existem dois os mecanismos de base:

- a localização que consiste saber a todo o momento onde se encontra um celular,
- a procura de um usuário (paging) que consiste em emitir mensagens de aviso de procura nas células onde o sistema havia localizado o usuário.

Zonas de localização – Zonas de localização agrupam um certo número de células. O sistema conhece a zona de localização (LA - Location Área) precisa do usuário, isto é, a ultima zona dentro da qual o celular sinalizou com a rede, mas ignora em qual célula ele se encontra dentro dessa zona. Logo que o usuário recebe uma chamada, o sistema procura o celular na LA emitindo um aviso de procura (mensagem paging) nas células da zona. Dessa maneira o consumo de recursos rádio será reduzido à procura do usuário dentro de uma zona de localização. A zona de localização é identificada por um endereço chamado "ponteiro de localização" ou "Location Pointer".

A atualização da localização do celular pode ser feita periodicamente pelo terminal, que emite em intervalos constantes, mensagens para a rede sinalizando sua posição. Entretanto, o método mais utilizado atualiza a localização no momento da passagem do celular de uma zona para outra LA. Cada estação de base BTS difunde periodicamente o número da LA ao qual ela pertence num canal rádio especifico (BCCH). Por sua vez, o celular que escuta periodicamente esse canal armazena em permanência o número da zona corrente. Se o celular percebe que o número da zona dentro da qual ele se encontra é diferente daquela que ele havia armazenado, ele sinaliza sua nova posição à rede (Figura 34). Esse mecanismo (location update procedure) é também chamado de "inscrição" ou "registramento". As bases de dados de localização da rede vão também ser atualizadas.

Um compromisso deve ser encontrado entre o custo das atualizações da localização e o custo da procura de usuários. Isso consiste em otimizar o tamanho das zonas de localização em função da taxa de chamadas entrantes, a velocidade media dos celulares, o tamanho das células e a arquitetura da rede.

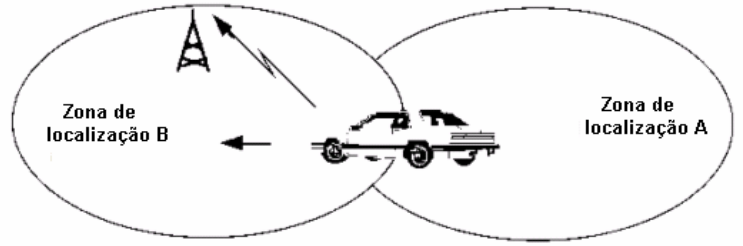


Figura 34 – Zonas de localização

5.4.1 Localização no GSM

O GSM combina os métodos de atualização periódica da localização e a atualização baseada na mudança da LA. Uma LA é identificada pelo endereço LAI (Location Área Identification), mostrado na Figura 35) composto dos elementos seguinte:

- MCC – indicativo do país, tal como no IMSI,
- MNC – indicativo do PLMN, tal como no IMSI,
- LAC (Location Área Code) – código da zona de localização livremente escolhido pelo operador (2 bytes no Maximo).

A identificação LAI determina de maneira única uma zona no seio do conjunto de PLMN do mundo. Ela permite ao celular detectar mudanças de zonas até mesmo aquelas devidas à mudança de PLMN.

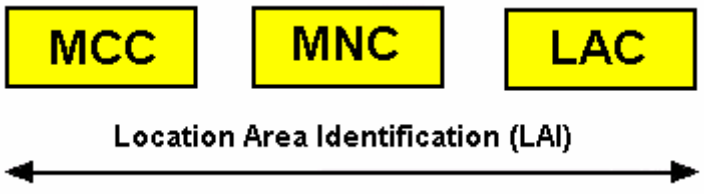


Figura 35 – Formato do LAI

5.4.2 Base de dados de localização no GSM

Um VLR pode gerenciar várias LA, entretanto uma LA não pode conter células dependentes de VLR diferentes. Para evitar a transferência inútil de sinalização só o VLR memoriza a LA corrente do conjunto de usuários que ele gerencia. O HLR memoriza a identificação do VLR corrente de cada usuário, mas não sua localização. A Figura 36 abaixo mostra as informações de localização contidas em cada entidade.

5.4.3 Atualização da Localização no GSM

Esse procedimento permite a rede transferir ao VLR o conjunto de características dos usuários presentes na zona controlada pelo VLR. Quando um celular não está em comunicação com a rede, ele escuta constantemente a identificação LAI da zona onde ele se encontra, armazena-a no chip SIM e lança um procedimento de atualização de localização se ele assim achar necessário. Para lançar esse procedimento o celular solicita à rede um canal rádio dedicado no qual não há outro usuário. Depois ele estabelece um certo número de conexões para poder trocar mensagens diretamente com o MSC. No final do procedimento a rede libera os recursos rádio utilizados durante o dialogo.

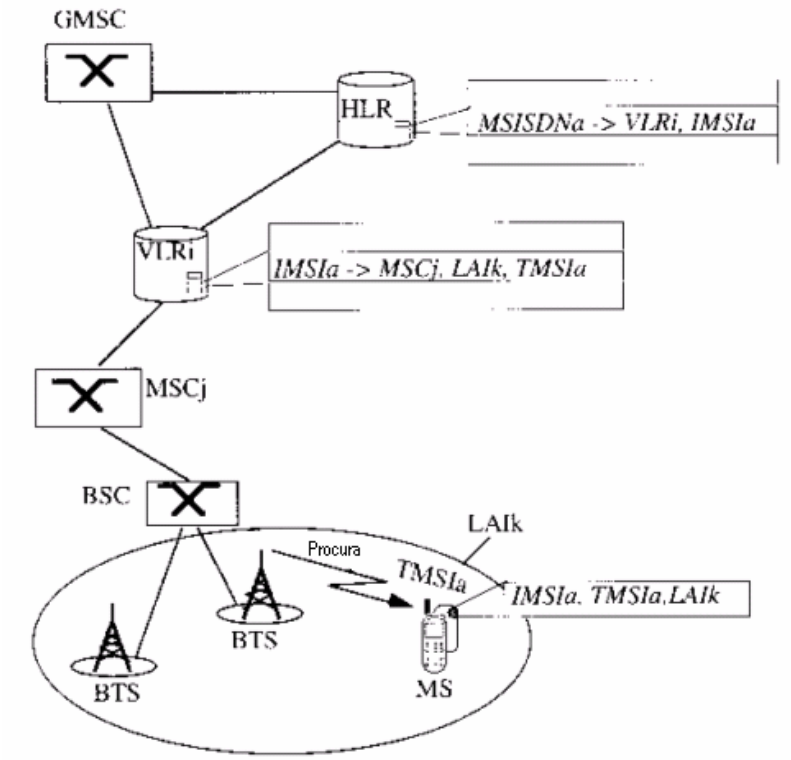


Figura 36 – Informações de localização

5.4.3.1 Atualização periódica:

A atualização periódica necessita que o celular no estado ligado (ON) mantenha um contato regular com a rede. O período de atualização é controlado pela rede que o difunde em um canal especifico (BCCH). Os valores possíveis estão compreendidos entre 6 minutos e 24 horas, sendo que o valor infinito anula a atualização periódica. Essa atualização é utilizada para corrigir possíveis incoerências de informações no seio da entidade da rede (por exemplo, panes de HLR, VLR ou conexões).

5.4.3.2 Procedimento IMSI Attach/Detach:

A fim de evitar procuras inúteis de celulares que foram colocados no estado desligado (OFF), o GSM define os procedimentos IMSI Attach (ON) e IMSI Detach (OFF). Nesse caso, os dados dos usuários no MSC/VLR contem um campo indicando se o celular pode ser encontrado (estado ligado) ou não (estado desligado).

O procedimento IMSI Detach é lançado no momento que o usuário desliga seu terminal ou retira o chip SIM do equipamento terminal. Em qualquer uma das dessas situações o equipamento permanece "ligado" o tempo suficiente para enviar ao MSC/VLR a mensagem IMSI Detach. A ativação deste último é uma escolha do operador porque ela não é forçadamente ótima em termos de sinalização gerada. Se um grande número de usuários desligarem seus celulares no final do dia, o procedimento IMSI Detach gerara um pico de tráfego que a rede terá dificuldade de escoar. Ainda mais, mesmo que esse procedimento evite a procura inútil de celulares desligados, durante a noite o ganho é muito pequeno.

O procedimento IMSI Attach é lançado no momento que o usuário liga seu terminal e tem por objetivo atualizar sua localização e sinalizar a rede que ele está de novo pronto para receber chamada. A localização é atualizada no VLR e se este não tem nenhuma informação sobre o usuário uma mensagem é enviada ao HLR solicitando as informações (direitos, dados de autenticação, etc) do usuário.

Se o VLR não tem contato com o celular durante um certo período (especificado por uma temporizarão) ele pode decidir de "detachar" o usuário marcando o celular como desligado. O VLR pode também apagar as informações de um usuário que não estabelece contato rádio durante um certo período determinado (vários dias, por exemplo). Essa operação se chama expiração dos dados do usuário. O VLR informa sobre essa operação ao HLR que armazena a indicação "MS purged" no registro de informações do usuário. Assim, toda chamada dirigida ao usuário é tratada como se este não pudesse ser encontrado na rede.

5.4.3.3 Procedimento de atualização da localização inter VLR

Logo que o celular é ligado (ON) ele deve se inscrever na rede. O celular envia ao MSC/VLR uma solicitação de localização. O MSC, através do IMSI, determina o HLR do usuário ao qual pode enviar um pedido de informações triplas se segurança e lançar um procedimento de autenticação do usuário. No caso de sucesso ele transmite ao HLR a mensagem MAP_LOCATION_UPDATE_REQUEST. O HLR envia ao VLR corrente as informações do usuário. O VLR envia um número TMSI ao celular através da mensagem TMSI_REALLOCATION_COMMAND. Esse procedimento é mostrado na Figura 37.

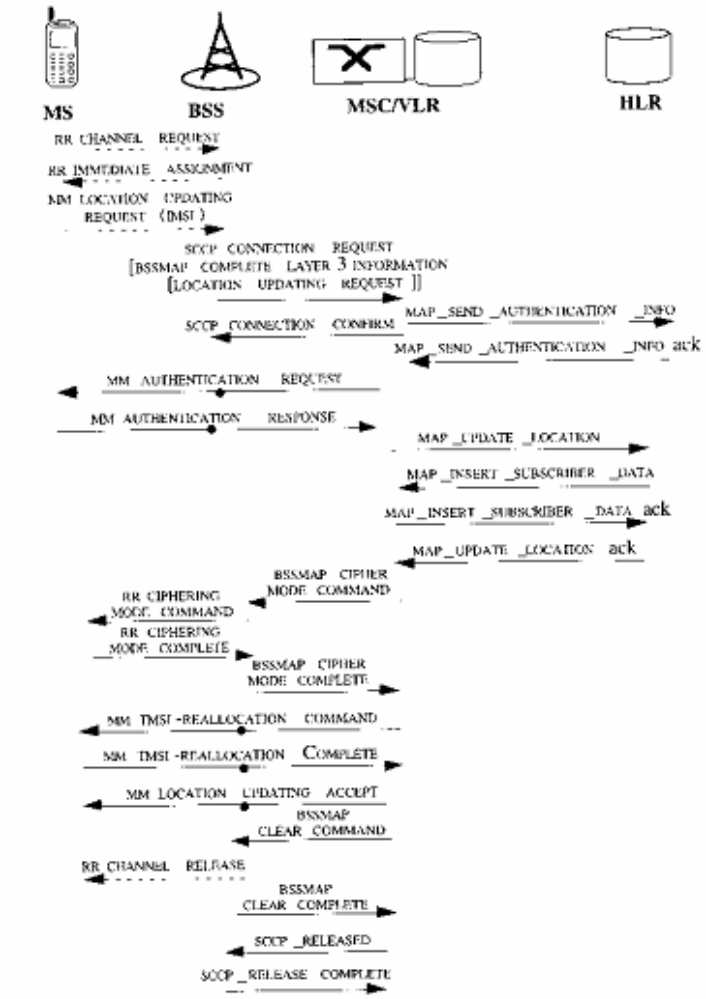


Figura 37 – Atualização da localização inter VLR

5.4.3.4 Procedimento de atualização da localização intra VLR

Logo que o telefone celular muda de LA, mas fica sob o mesmo VLR, a atualização é simples. A informação de localização é modificada somente no VLR e assim não são trocadas

mensagens de sinalização envolvendo MS, BSS, MSC e VLR. Nesse caso, a rede pode autenticar o usuário, conservando ou trocando seu TMSI. Esse procedimento é mostrado na Figura 38.

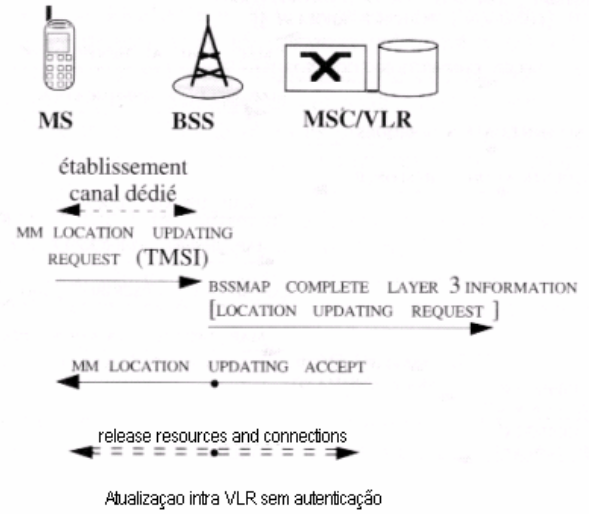


Figura 38 – Atualização da localização intra VLR

5.4.3.5 Atualização da localização Internacional

Essa atualização acontece no caso de um terminal de uma PLMN 1 (chamada de HPLMN) que visita uma PLMN 2 (camada VPLMN). De maneira idêntica às atualizações precedentes o celular lança o procedimento de atualização de localização. O terminal envia seu IMSI ao MSC (chamado de VMSC) que deve contatar o HLR do usuário na rede HPLMN. Para isso o MSC utiliza os campos MCC e NDC do IMSI e a rede internacional SS7 para troca de mensagens com o HLR. Ao final, o VMSC/VLR armazena as informações do usuário e o HLR memoriza o endereço do VLR onde o usuário está registrado. A Figura 39 ilustra esse procedimento.

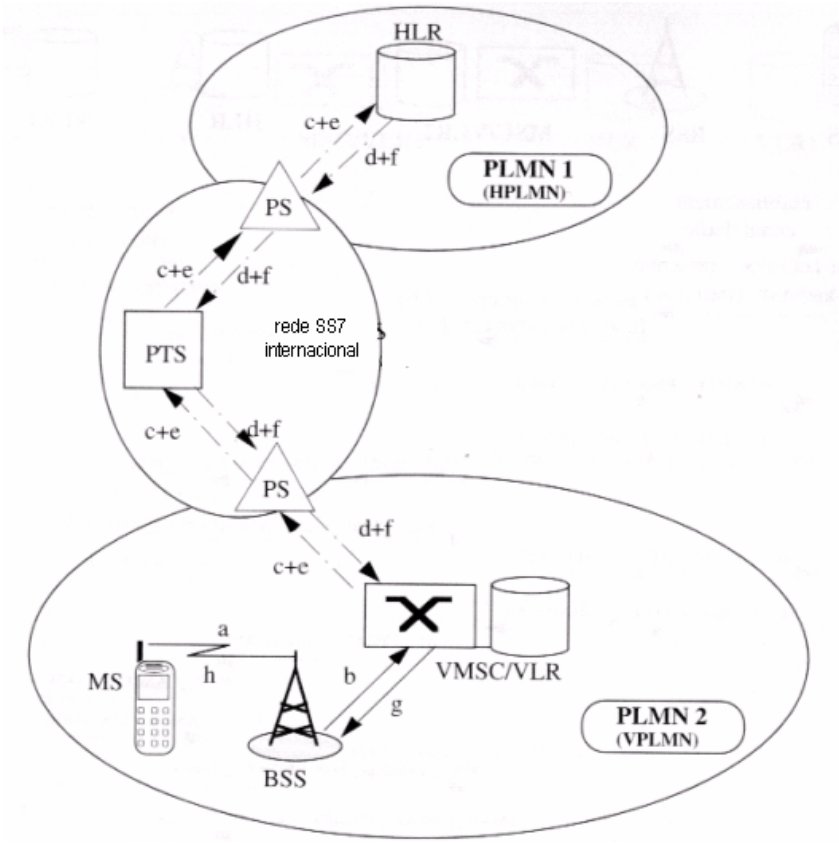


Figura 39 - Atualização da localização Internacional

5.4.4 Atualização devido à mudança de célula

Existem três casos de mudança de célula devido ao movimento de um usuário dentro da zona de cobertura de uma PLMN.

5.4.4.1 Mudança de célula dentro da mesma LA.

A Figura 40 abaixo ilustra o caso de um celular que muda sua localização passando de uma célula para uma célula vizinha dentro da mesma LA. Neste caso, verificamos as três fases seguintes:

Fase 1: O celular escuta o canal de difusão BCCH (IT0 da f0 da BTS) da BTS 1 e verifica que ele está na zona LA1.

Fase 2: O Celular se afasta da BTS 1

Fase 3: O celular escuta o BCCH da BTS 2 e verifica que a zona é a LA1 e portanto não precisa fazer a atualização de sua localização.

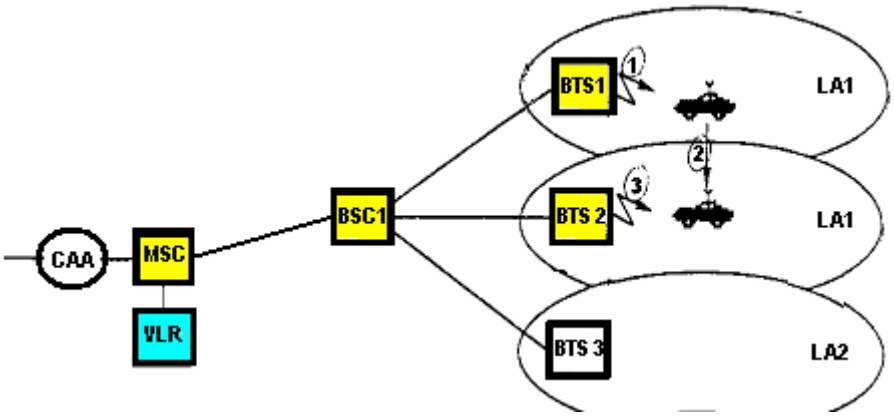


Figura 40 - Mudança de célula dentro da mesma LA

5.4.4.2 Mudança de célula e de LA.

A Figura 41 abaixo ilustra o caso de um celular que muda sua zona de localização quando de desloca de uma célula para uma célula vizinha. O processo de atualização da localização é realizado conforme as fases seguintes:

Fase 1: O celular escuta o canal de difusão BCCH (IT0 da f0 da BTS) da BTS 2 e verifica que ele está na zona LA1. Ele escuta também as células vizinhas procurando uma melhor escolha para a transmissão.

Fase 2: O Celular se afasta da BTS 2

Fase 3: O celular escuta o BCCH da BTS 3 e verifica que a zona é a LA2, diferente da LA 1. Ele então sinaliza ao VLR que ele está agora na zona LA2.

Fases 4 a 7 : O celular faz uma solicitação de atualização de localização ao VLR que o autentica e troca sua localização de LA1 para LA2.

Fases 8 a 11 : O VLR confirma a atualização e envia ao celular um TMSI.

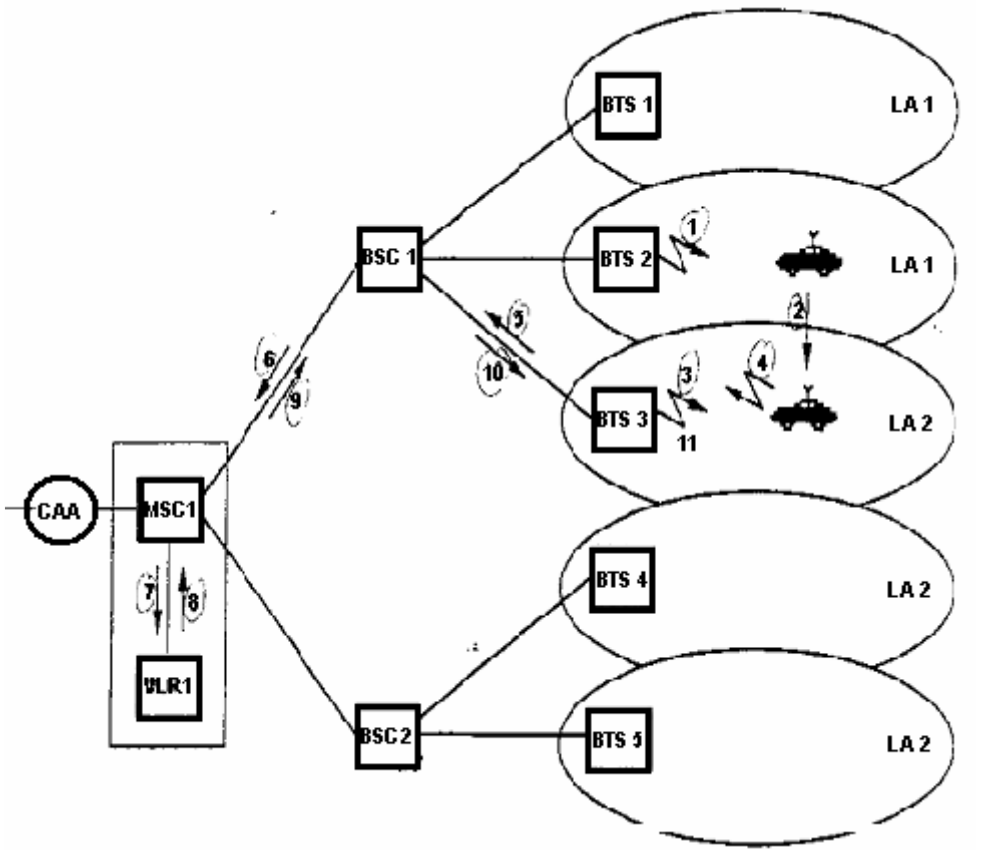


Figura 41 - Mudança de célula e de LA

5.4.4.3 Mudança de célula e de zona de comutação

A Figura 42 abaixo ilustra o caso de um celular que muda sua zona de comutação quando de desloca de uma célula para uma célula vizinha. O processo de atualização da localização é realizado conforme as fases seguintes:

Fase 1: O celular escuta o canal de difusão BCCH (IT0 da f0 da BTS) da BTS 6 e verifica que ele está na zona LA2. Em seguida ele escuta as células vizinhas procurando uma melhor escolha para a transmissão.

Fase 2: O celular se afasta da BTS 6.

Fase 1: O celular escuta o BCCH da BTS 7

Fase 4 a 7: O celular envia uma solicitação de atualização de localização ao VLR 2. O HLR é dado pelos dígitos H1H2 do IMSI.

Fase 8 a 11: O VLR 2 recupera as 5 informações triplas, os dados do usuário são copiados no VLR2, o usuário é autenticado, o HLR atualiza suas informações (troca VRL1 por VLR2), o VLR 2 atualiza as informações do usuário.

Fase 12 a 15: Confirmação da nova localização e novo TMSI.

Fase 16: Apagamento de todas as informações sobre o usuário do VLR1.

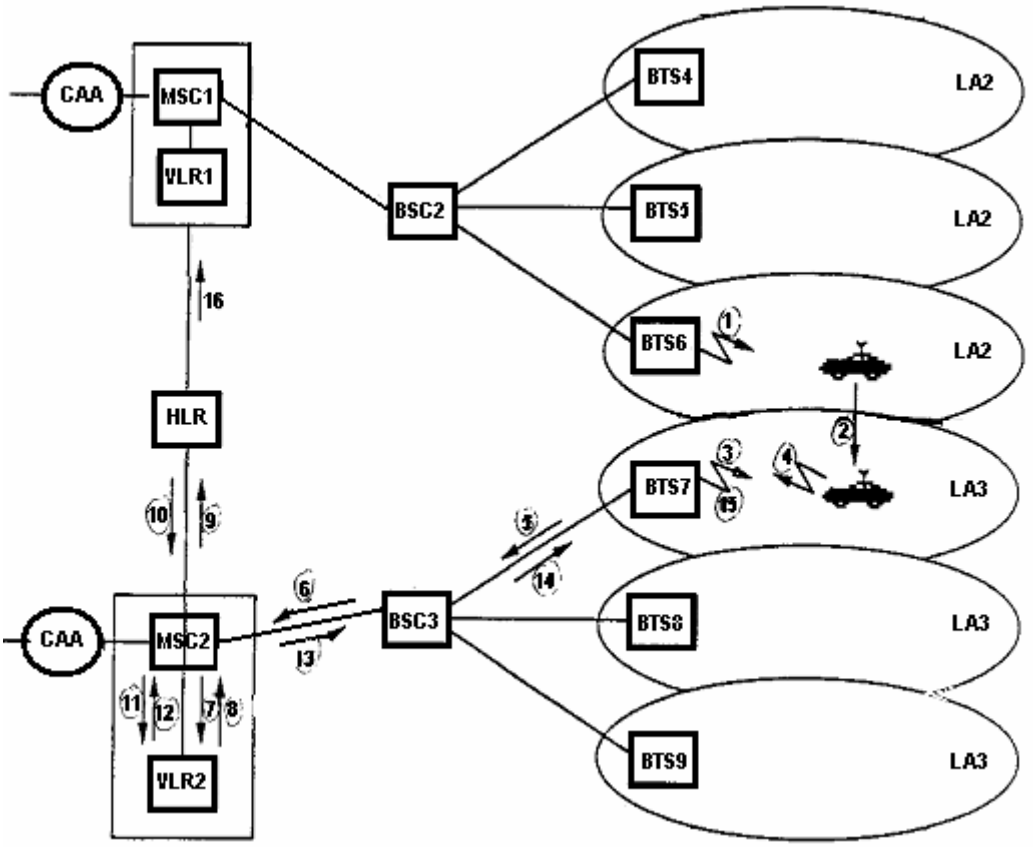


Figura 42 - Mudança de célula e de zona de comutação

5.5 Tipos de chamada

5.5.1 Chamadas entre fixo e celular

Chamada originada (de Celular para fixo) - Para originar uma chamada o usuário de uma PLMN digita o número desejado e comanda o inicio da chamada a partir de seu terminal. Ao contrario da rede fixa, no GSM a digitação do número do chamado é dita "off-line". Logo que a chamada é validada, o celular solicita à rede um canal rádio a fim de trocar mensagens de sinalização. Ele envia a mensagem CN SERVICE REQUEST com a identificação TMSI ou IMSI, o tipo de serviço desejado e as informações necessárias. A rede autentica o usuário e aciona a criptagem. O celular envia o número do usuário chamado. O VMSC trata a chamada como uma chamada telefônica qualquer. Um canal rádio de tráfego é alocado e o celular é comutado sobre esse canal. Logo que o usuário chamado atende, a comunicação é estabelecida. O tempo típico que leva esse procedimento, mostrado na Figura 43, é de 6 segundos.

A comunicação entre o VMSC e o CAA (Central Automática de Assinantes) pode ser feita através da RTCP. Neste caso uma grande parte da comunicação utiliza os equipamentos de outro operador, ficando o operador da PLMN obrigado a pagar a correspondente fração da comunicação a esse operador. O operador da PLMN pode utilizar CT próprias a fim de encaminhar a chamada até o CAA do usuário chamado, diminuindo os custos da comunicação.

Chamada terminada (de Fixo para Celular) – Para originar a chamada o usuário da rede fixa digita o MSISDN do usuário móvel com quem ele quer se comunicar. Os primeiros dígitos do MSISDN identificam a PLMN do usuário chamado. A chamada é encaminhada até o GMSC através dos comutadores da rede telefônica. O GMSC interroga o HLR a fim de conhecer a localização do celular. O HLR procura o IMSI e o VLR ao qual o usuário está registrado, depois solicita a esse VLR um número MSRN (o VLR memoriza esse número). O GMSC pode agora estabelecer um circuito telefônico clássico com o VMSC utilizando para isso o MSRN

como número de chamada. O VMSC/VLR utiliza esse MSRN para descobrir o IMSI, a LA do celular e o seu eventual TMSI. O VMSC difunde uma mensagem "paging" contendo o TMSI nas células da zona de localização. O celular efetua um acesso na célula onde ele se encontra e o BSC lhe aloca um canal dedicado para troca de sinalização. Após o procedimento de autenticação e criptagem a mensagem de chamada é enviada ao celular, estabelecendo-se a comunicação, como mostrado na Figura 44.

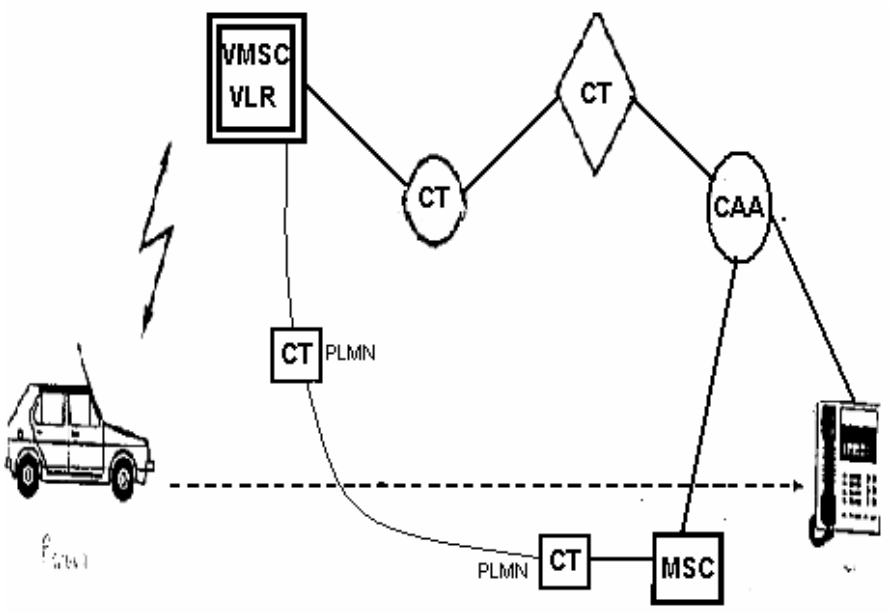


Figura 43 – Chamada originada

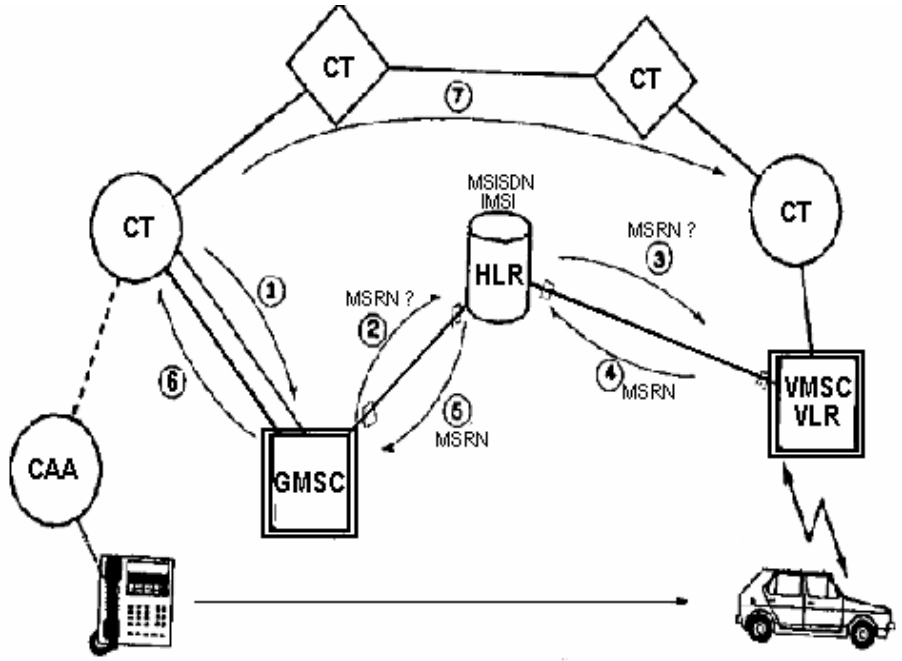


Figura 44 – Chamada terminada

Chamada originada e terminada internacional – A Figura 45 abaixo (esquerda) mostra o cenário de encaminhamento de uma chamada originada por um usuário móvel para um usuário fixo internacional. A Figura 45 da direita mostra uma chamada originada por um usuário (fixo) internacional para um usuário móvel.

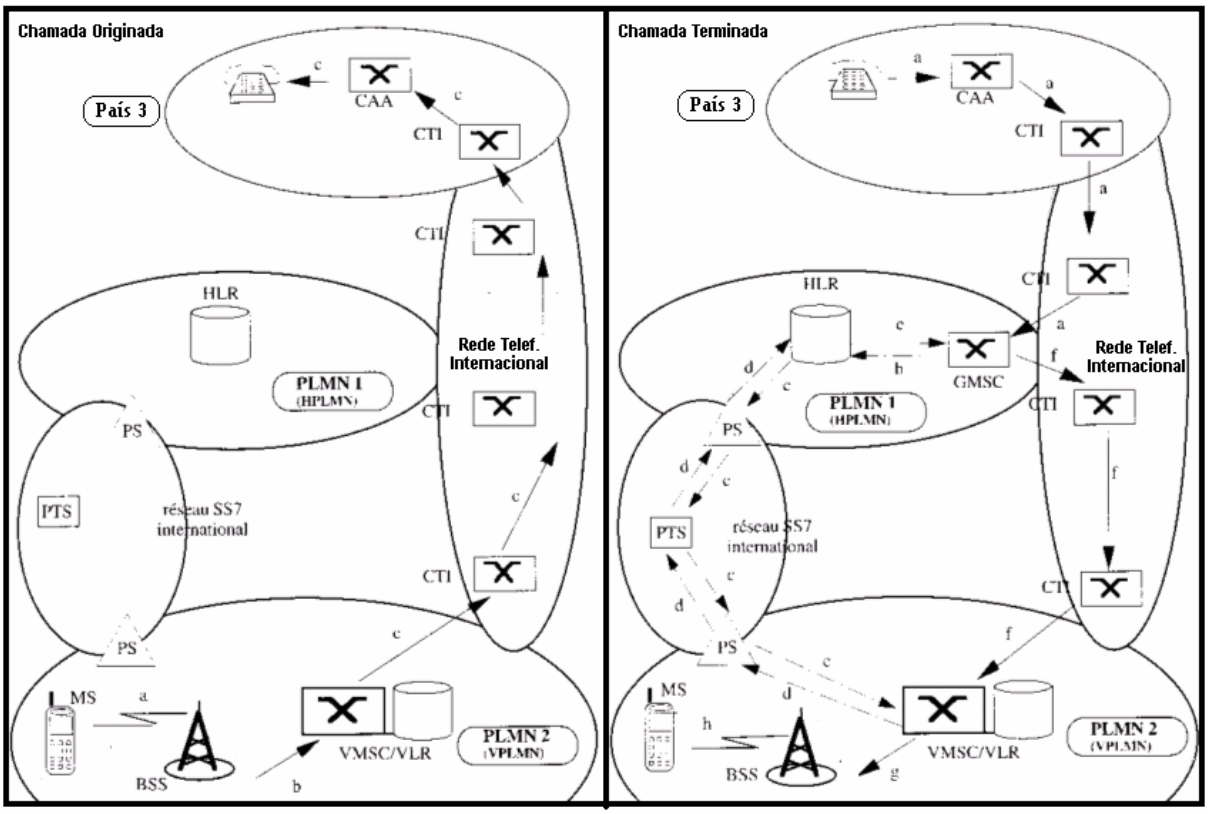


Figura 45 - Chamada originada e terminada internacional

5.5.2 Chamadas entre Celulares

As Figura 46, Figura 47 e Figura 48 abaixo ilustram três casos possíveis de chamadas originadas de um celular para outro celular.

Caso 1 – Neste caso os dois celulares pertencem à mesma PLMN.

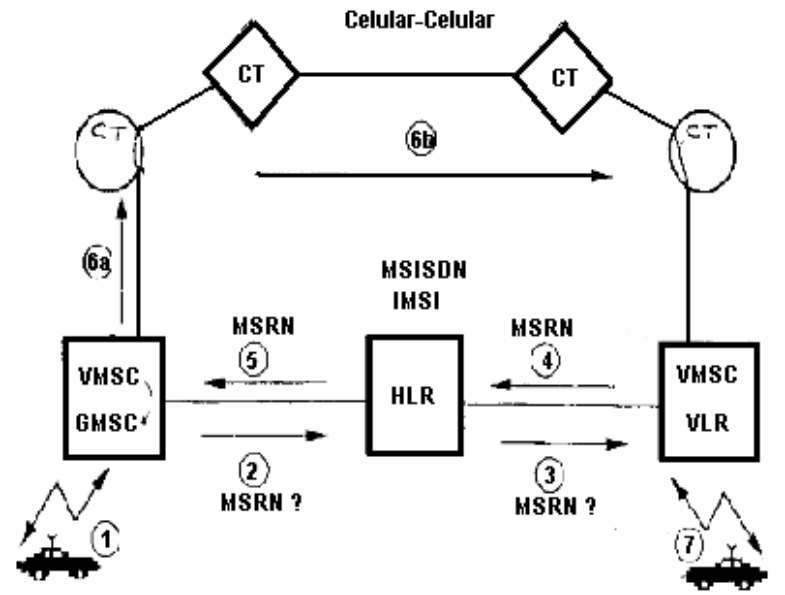


Figura 46 - Celulares da mesma PLMN

Caso 2 – Neste caso os celulares pertencem a PLMN diferentes.

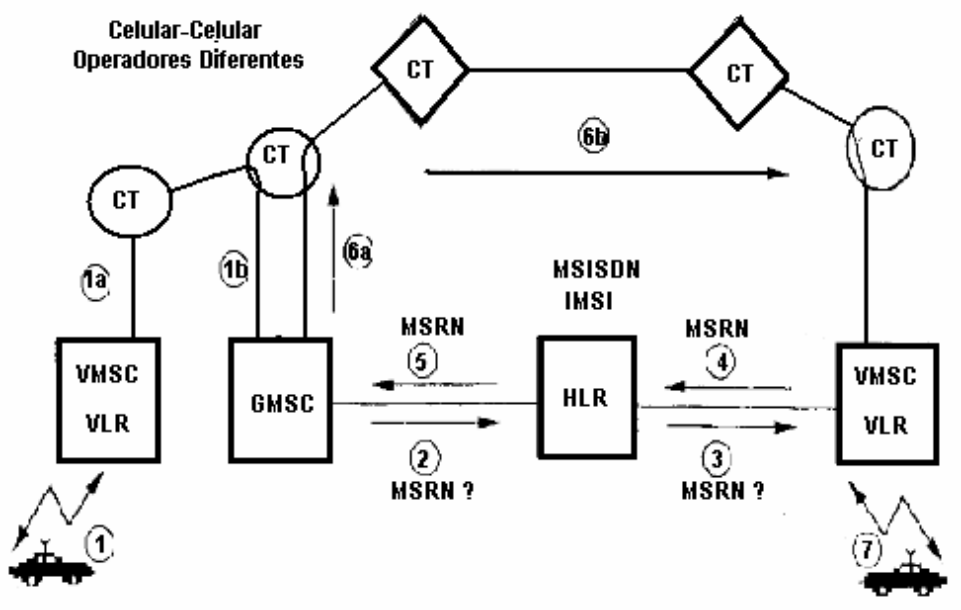


Figura 47 - Celulares de PLMN diferentes

Caso 3 – Neste caso os celulares estão em um país diferentes do país de sua PLMN. Na esquerda da Figura 48 verificamos que o circuito de voz fica estabelecido entre os MSC dos dois paises. Isso é conhecido por efeito "trombone". Para evitar esse efeito o sistema GSM especificou o roteamento SOR (Support of Optimal Routeing), como mostrado na direita da Figura 48.

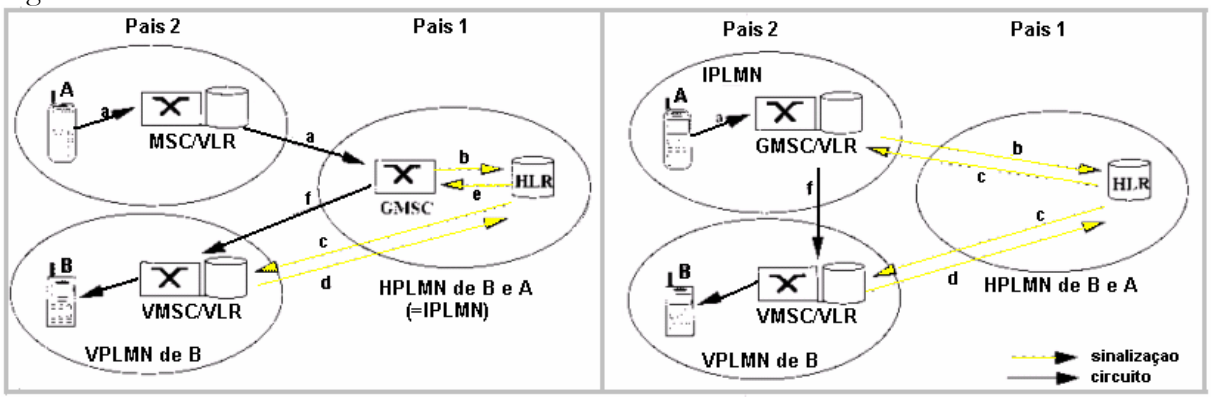


Figura 48 - Celulares em países diferentes

5.6 Handover

O Handoevr é a funcionalidade que permite ao usuário em comunicação de se deslocar e mudar de célula sem, contudo perder a sua conexão. Desde que um celular em comunicação sai de sua célula, o handover permite assegurar a continuidade de sua comunicação lhe afetando um novo canal rádio e re-encaminhando o circuito de voz para a estação da nova célula.

5.6.1 Handover intra BSC

Neste tipo de handover, o celular se desloca e troca de BTS sem, contudo trocar de BSC. As fases do procedimento desse handover são mostradas na Figura 49 abaixo.

Fase 1 – O celular está em comunicação com a BTS 2.

Fase 2a – O celular envia as medidas (efetuadas no sentido "down") Rx Lev e Rx Qual das 6 células adjacentes elegíveis.

Fase 2b – A BTS envia ao BSC as medidas recebidas em 2a e as medidas por ela efetuada (Rx Qual, Rx Level e a distancia d). Após a analise dos dados, o BSC decide o handover e escolhe a melhor BTS (BTS 3).

Fase 3 – O celular se desloca.

Fase 4a, 4b – O BSC reserva um canal rádio na BTS 3.

Fase 5a, 5b – O BSC informa ao celular sobre o canal escolhido.

Fase 6a, 6b – O celular faz o "Handover Access" (4 tentativas) para se conectar através do novo canal.

Fase 7 – A rede comuta o circuito de voz para a BTS 3.

Fase 8 – A rede libera o canal da BTS2.

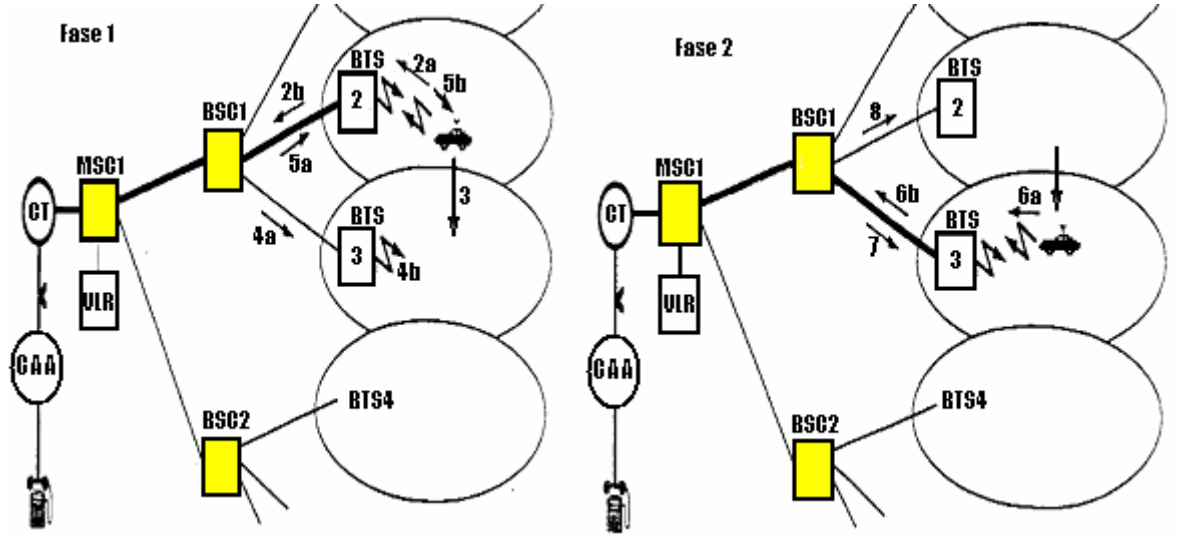


Figura 49 - Handover intra BSC

5.6.2 Handover intra MSC

Neste tipo de handover, o celular se desloca e troca de BTS e de BSC como mostrado na Figura 50 abaixo. O BSC1 decide de executar o handover do celular. Ele se endereça ao MSC1 a fim de solicitar a reserva do canal rádio na BTS 4 que é controlada pelo BSC 2. Este envia ao MSC1 todas as informações sobre o novo canal rádio reservado para o handover. O MSC1 envia essas informações ao celular que acessa ao novo canal como no caso precedente. O BSC2 informa ao MSC1 que o acesso foi efetivado. O MSC1 comuta o circuito de voz para o BSC 2 e BTS 4.

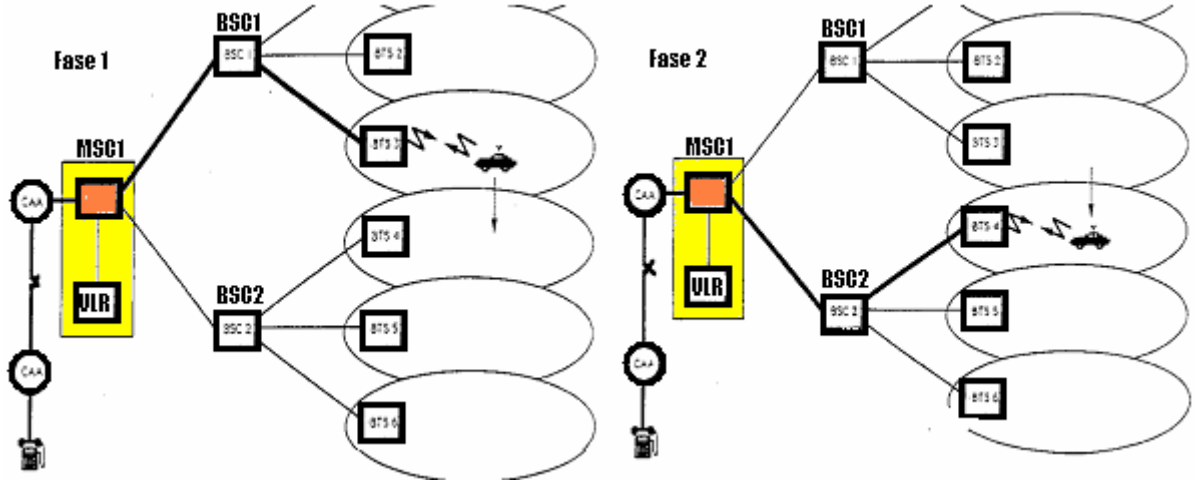


Figura 50 - Handover intra MSC

5.6.3 Handover inter MSC

Neste tipo de handover, o celular se desloca e troca de BTS, de BSC e de MSC como mostrado na Figura 51 abaixo. As etapas do handover são as seguintes:

- Inicialmente o celular está em comunicação com o MSC1, BSC1 através da BTS6, mas se desloca para a célula vizinha BTS7 (fase 2).
- Nas fases 4, 5a, 5b e 5c um canal rádio é reservado para o celular na BTS7.
- Na fase 6 o MSC2 informa ao MSC1 que o canal foi reservado.
- Nas fases 7a, 7b e 7c é enviada ao celular a indicação do novo canal que o celular deve utilizar.
- O celular realiza o acesso ao novo canal ("handover acesss") nas fases 9a, 9b e 9c.
- Na fase 9d o MSC2 informa ao MSC1 que o acesso ao novo canal foi realizado.
- Tendo sido realizado o acesso ao novo canal rádio, a circuito de voz é comutado na fase 10.
- Nas fases 11a, 11b e 11c o canal da BTS6 é liberado.

O MSC1 continua no circuito de voz qualquer que seja o deslocamento do celular, pois isso permite uma taxação unicamente a partir do MSC1. Durante a comunicação, qualquer que seja o deslocamento do celular, o usuário não muda de VLR (VLR1), sendo a nova localização atualizada no final da comunicação.

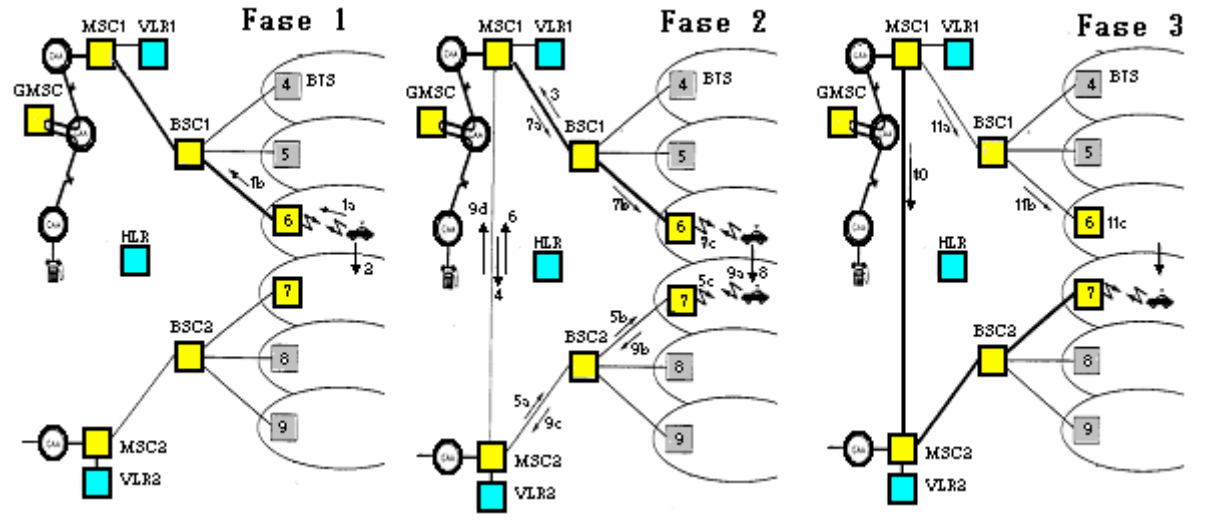


Figura 51 - Handover inter MSC

Unidade 6 A interface rádio GSM

A transmissão no GSM é assegurada pela interface rádio, uma das partes mais sofisticada e rica em funções do sistema.

6.1 Compartilhamento de recursos rádio

Um sistema de comunicação móvel necessita de um espectro de radiofreqüência para funcionar. Os projetistas dos sistemas devem solicitar uma banda de freqüência aos organismos oficiais encarregados da gerencia do espectro de freqüência. Se o sistema tem por objetivo operar ao nível internacional, a banda de freqüência deve ser alugada ao nível do IUT. As bandas de freqüência dedicada pelo IUT ao sistema GSM e sua extensão DCS são especificadas na Tabela 11 abaixo.

	GSM	DCS-1800
Banda de freqüência	890-915 up 935-960 down	1710-1785 up 1805-1880 down
Largura (2 x W simplex)	2 x 25 MHz	2 x 75 MHz
Ecarte (delta W duplex)	45 MHz	95 MHz

Tabela 11 – Bandas de freqüência

6.1.1 Compartilhamento em freqüência

A banda dedicada ao GSM é dividida em bandas de freqüências com largura de 200KHz. Numa banda de freqüência são emitidos sinais modulados em torno de uma freqüência portadora no centro da banda.As freqüências são alugadas de uma maneira fixa as BTS e são designadas de maneira geral como "portadoras" ou ARFC (Absolute Rádio Frequency Channel). É necessário verificar que duas BTS vizinhas não utilizem portadoras idênticas ou próximas.

6.1.2 Compartilhamento em tempo

Cada portadora é dividida em intervalos de tempo (IT) chamados slots. La duração de uma slot foi fixada no GSM em:

$$T_{slot} = (75/130)*0.001 \text{ s, ou seja, } 0.5769 \text{ ms ou } 577\mu s.$$

Um slot transporta um elemento de sinal radioelétrico chamado burst. O Acesso TDMA permite a diferentes usuários compartilhar uma dada banda de freqüência. Em uma mesma portadora slots são agrupados em número de 8 formando tramas TDMA. A duração de uma trama TDMA é então de:

$$T_{TDMA} = 8 * T_{slot} = 4.6152 \text{ ms}$$

Cada usuário utiliza um slot por trama. Os slot são numerados por um índice TN que varia de 0 a 7. Um canal físico é então constituído pela repetição periódica de um slot dentro da trama TDMA em uma freqüência particular. Entretanto, os projetistas do GSM previram a possibilidade de alugar a um usuário um só slot a cada duas tramas TDMA. Essa alocação constitui um canal físico de meia taxa de transmissão. OS canais físicos de meia taxa de transmissão serão utilizados com o aparecimento dos codificadores de voz de grande performance.

Podemos dizer que o GSM é um sistema F/TDMA, porque os recursos rádio são compartilhados em freqüência e em tempo. Entretanto costumamos referenciar o GSM como um sistema TDMA. A Figura 52 abaixo ilustra tramas TDMA e canais físicos de plena e meia taxa de transmissão.

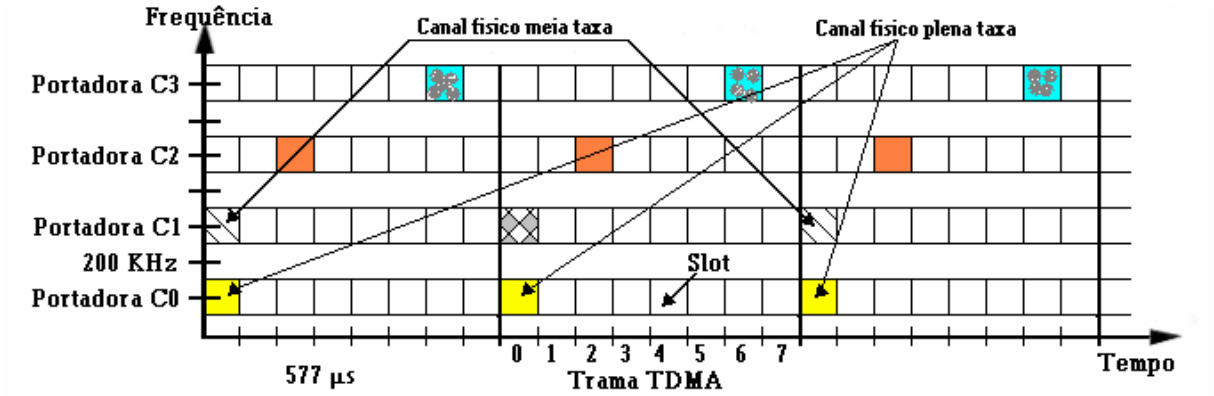


Figura 52 – Canais físicos meia e plena taxa

6.1.3 Salto de freqüência

A opção do salto de freqüência lento (SFH – Slow Frequency Hopping) aumenta a capacidade do sistema GSM. Ela permite lutar contra o "fading" seletivo (heterogeneidade de freqüência) e gerenciar melhor as interferências. A combinação da técnica TDMA e do salto de freqüência é chamada FH/TDMA.

Normalmente o salto de freqüência não é ativado durante a fase de implantação da rede, quando o tráfego não é ainda tão intenso. Logo que o salto é ativado, um canal físico não reside mais sobre uma só freqüência, mas utiliza um conjunto de portadoras que são percorridas segundo uma ordem definida para o salto de freqüência, como mostra a Figura 53 abaixo. Essa seqüência é definida sobre um conjunto N de freqüências atribuídas a BTS. A seqüência pode ser cíclica de período N onde as freqüências são percorridas dentro de uma ordem regular ou pode ser pseudo-aleatória com período máximo igual a N. O máximo valor de N permitido é 64.

As freqüências sobre as quais o salto é realizado são numeradas de 0 a N-1. Um algoritmo definido na norma gera uma serie pseudo-aleatória de números Si compreendidos entre 0 e N-1. O algoritmo utiliza como argumento o número da trama FN e um parâmetro HSN (Hoppinh Sequence Number) compreendido entre 1 e N-1. No momento da alocação de um canal, a BTS indica ao celular um índice MAIO (Mobile Allocation Index Offset) compreendido entre 0 e N-1. O celular determina o número da freqüência a utilizar somando (modulo N) o índice MAIO ao número Si. Assim, para um dado slot os N valores possíveis do índice MAIO definem N canais físicos deferentes dentro da mesma BTS.

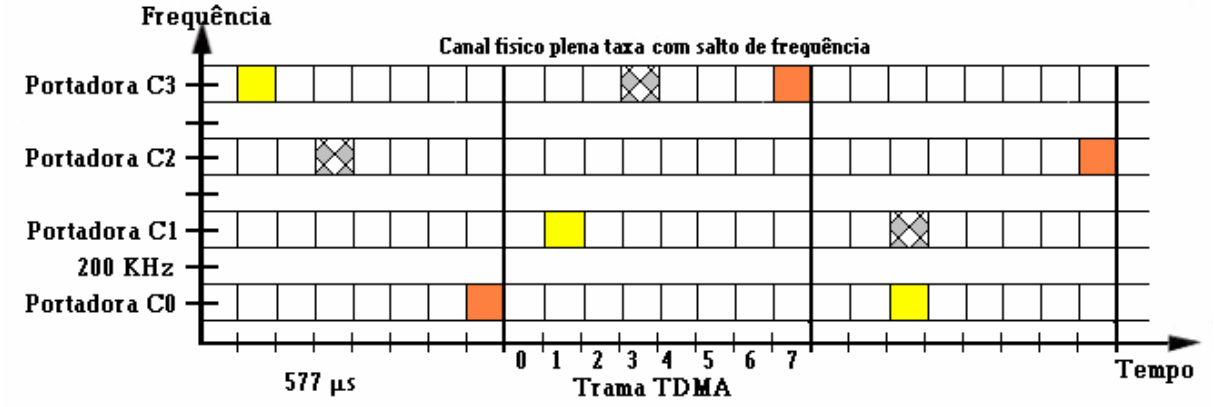


Figura 53 – Salto de freqüência

6.1.4 Canal físico duplex

No GSM a banda total alocada ao sistema é separada em duas sub-bandas separadas por um intervalo de freqüência que não é atribuída ao sistema. Essa separação entre as bandas "up" e "down" facilita a filtragem e a separação dos canais. Essa separação é 45MHz no GSM e de 95MHz no DCS.

Um canal físico simplex se refere a um slot por trama TDMA sobre uma portadora (sem salto de freqüência). Um canal físico duplex corresponde a dois canais simples. Se a portadora do canal de descida (down) é fd(i) e a separação é dW_{duplex}, o canal de subida (up) está na freqüência fu(i) onde:

$$fu(i) = fd(i) - dW_{duplex}$$

Logo, um canal físico corresponde ao recurso necessário para uma comunicação telefônica.

No GSM o celular emite e recebe em instantes diferentes, sendo a emissão e a recepção deslocadas de uma duração correspondentes a 3 (três) slots. Para conservar a numeração (TN) de 0 a 7 dos slots a sincronização da trama de subida é deslocada também de $3*T_{slots}$ conforme a Figura 54 abaixo. Esse deslocamento permite simplificar o filtro presente dentro de cada celular. Seu objetivo é rejeitar o sinal proveniente de uma outra eventual estação próxima emitindo durante a fase de recepção do celular.

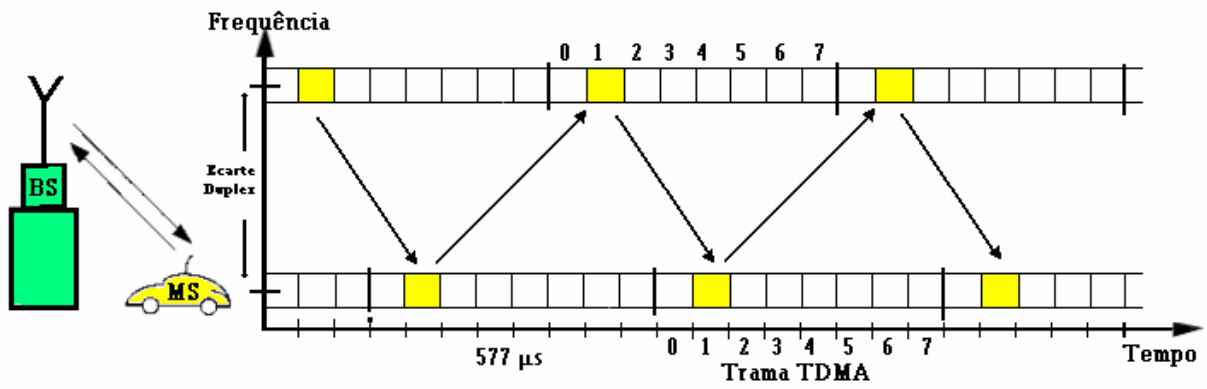


Figura 54 – Canal físico duplex

6.1.5 Numeração das portadoras

Cada portadora é identificada de maneira única por um número chamado ARFCN codificado por 10 bits. O plano abaixo apresenta a identificação das portadoras no sentido "down" (em MHz) :

- para 1 <= n <= 124 fd = 935 + (0.2 * n) (GSM)
- para 512 <= n <= 885 fd = 1805.2 + (0.2 * (n-512)) (DCS)

O número das portadoras no sentido "up" é calculado utilizando-se o "écarte" duplex. O número total de portadoras Nc para um sistema é igual a:

- Nc = 124 para o GSM,
- Nc = 375 para o DCS,

O número de canais físicos duplex é dado por 8 * Nc.

6.1.6 Compensação do tempo de propagação

Os diferentes usuários de um sistema celular estão em distancias variáveis de suas estações de base proporcionando retardos de propagação das transmissões τ_p variáveis. Por exemplo, 30Km são percorridos em 100µs. É necessário impedir que dois celulares que utilizem dois slots consecutivos enviem bursts que se superponham no receptor da BTS. Como mostra a Figura 55 abaixo, a MS1 utiliza o slot 1 para enviar seus bursts enquanto que a MS2 utiliza o slot 2. Devida a grande distancia entre a MS1 e a BTS, o burst enviado por esse celular chega ao receptor da BTS superposto no tempo ao burst enviado pela MS2.

Para evitar esse problema duas soluções possíveis são:

- 1- aumentar o tempo de guarda (guard time) ou tempo de silencio entre o final do burst e o final do slot;

– 2- compensar o tempo de propagação de ida e volta gerenciando o parâmetro TA (Time Advance). O celular que se encontra mais longe da BTS deve avançar a emissão de cada um de seus slots de uma tempo τ_p com relação ao instante inicial do slot, ou seja, $2*\tau_p$ com relação ao relógio que ele recebe.

No GSM o tempo de guarda foi estabelecido em 30 μs e os retardos maiores são compensados pelo parâmetro TA

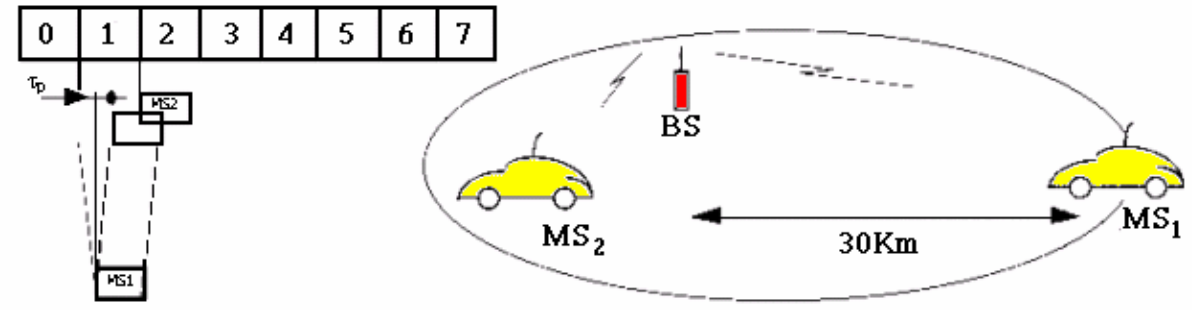


Figura 55 – Compensação do tempo de propagação

6.1.7 Transmissão da voz

O sinal analógico de voz, que no caso pode ser visto como uma função x(t) com espectro limitado entre 300 e 3400Hz, é amostrado em intervalos de 20 ms. Cada intervalo é digitalizado, comprimido (pelo codificador de voz) e protegido (pelo codificador de canal) para resultar em uma trama codificada chamada de bloco de 456bits. Essa digitalização introduz um retardo de 20ms, pois para tratar uma amostra correspondente a 20ms de voz é necessário tê-la recebido totalmente.

Uma vez recebido o bloco de voz digitalizada, comprimida e protegida é necessário pensar na sua transmissão. A solução mais simples seria dividir o bloco de 456 bits em 4 bursts de 114 bits e os enviar dentro de 4 tramas TDMA consecutivas. Entretanto o GSM procura repartir ao máximo a transmissão do pacote de voz no tempo. O pacote é repartido e transmitido dentro de oito tramas TDMA. Cada meio burst do pacote de voz número i é combinado com um meio burst do pacote de voz número i-1 ou com um meio burst do pacote de voz número i+1.

A Figura 56 abaixo ilustra o processo de digitalização e transmissão de blocos de voz de 20ms.

6.1.8 Transmissão de dados

A transmissão de dados e de sinalização pode ser descrita da mesma forma que a transmissão de voz. Por exemplo, no caso de um fluxo de 9600 bits/s 48 bits são transmitidos durante 5 ms. A esses 48 bits são anexados 12 bits de controle para formar um bloco de 60 bits. Quatro blocos são agrupados para formar um bloco de 240 bits a cada período de 20 ms.Isso significa uma taxa de 12 kbit/s.

O conjunto de tratamentos descrito para a voz (codificação e proteção, entrelaçamento, criptografia, ..) são aplicados também para a transmissão de dados e de sinalização.

6.1.9 Modulação GMSK

A modulação utilizada no GSM é a modulação GMSK (Gaussian-filered MSK). A taxa binária em linha é de 270.833 Kbis/s. A norma GSM define o gabarito que o espectro do sinal deve respeitar para os diferentes equipamentos. A Figura 57 abaixo ilustra o gabarito do espectro do sinal emitido pelo celular.

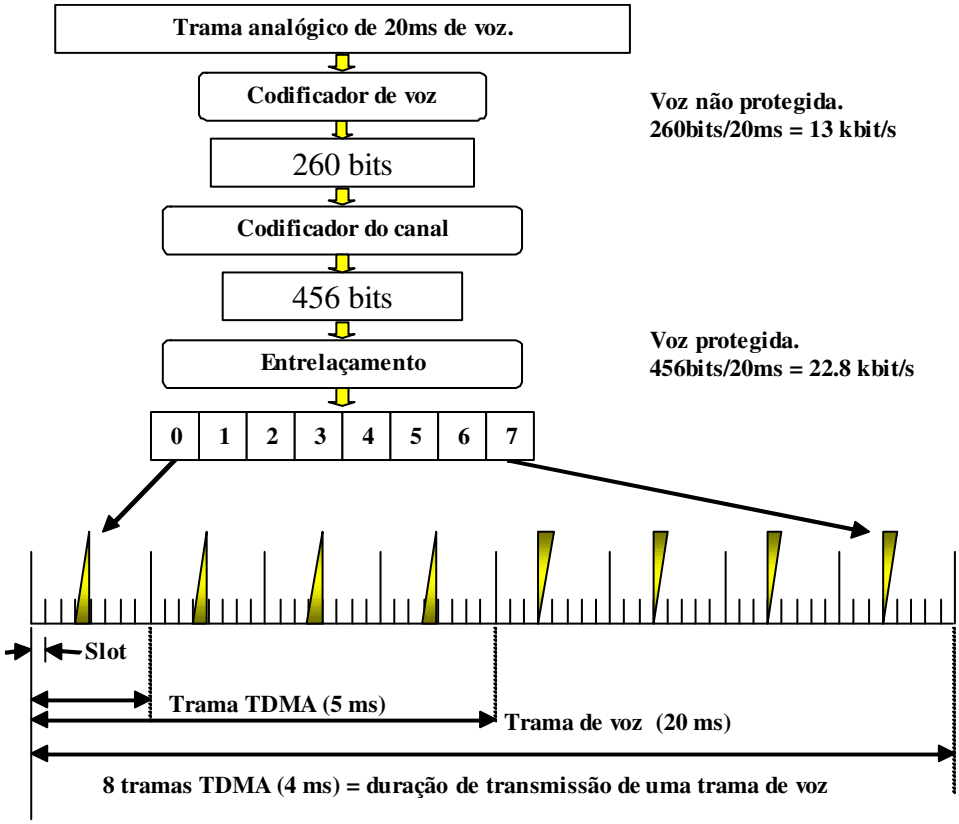


Figura 56 - Transmissão da voz

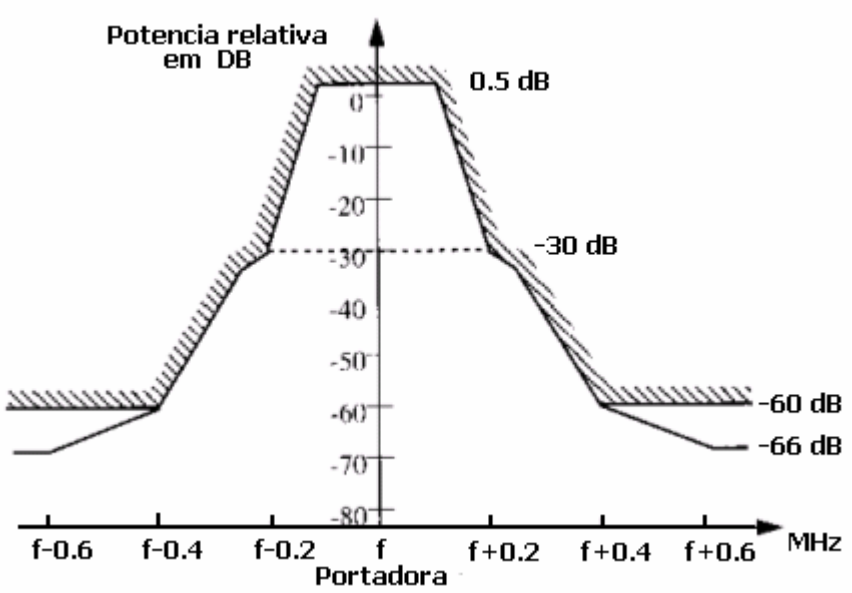


Figura 57 - Modulação GMSK

6.1.10 Formato do burst

O formato de um burst normal é mostrado na Figura 58 abaixo. Cada trama consiste de um certo número de bits. Esses bits são organizados seguindo uma estrutura que difere em função do protocolo utilizado para cada slot e do estado desse protocolo. Um slot, cuja duração é de 0,5769 ms, pode transportar 156.25 bits dos quais 114 bits de mensagem. Admitindo que os slots são enviados sem interrupção, temos que a taxa máxima de transmissão é de 270.833 kbit/s (cálculo: 156.25/0.5769). Na pratica a taxa útil máxima (em modo full-rate) não ultrapassa 13

kbits/s em razão dos bits necessários a correção de erros. Para a transmissão de dados esta taxa cai para 12 Kbits/s.

Todos os tipos de burst têm uma forma semelhante. Eles são compostos de:

- Três (3) bits de cabeçalho, chamados de"tail bit" ou TB, necessários a sincronização. Eles correspondem ao código 000 (exceto nos bursts de acesso).
- 148 bits úteis cujo formato depende do tipo de burst.
- Três (3) bits de fim também chamados do "tail bit".
- 8.25 bits (ou 30.5 µ) de tempo de guarda correspondente à diferença de duração de um burst e de um slot. Esse período temporal tem as seguintes funções:
  - Permitir que o emissor do burst reduza sua potencia de 70 dB, conforme o gabarito especificado pela norma. Esse gabarito tem por objetivo assegurar que dois bursts emitidos dentro de slots consecutivos não superponham suas partes úteis.
  - Compensar a variação da duração de transmissão de pacotes enviados por um celular que está em movimento.

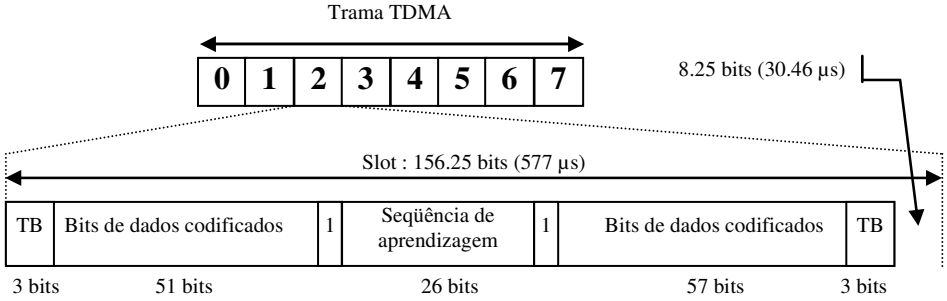


Figura 58 – Formato do burst normal

Outros quatro tipos de pacotes funcionais, chamados de "burst" na terminologia GSM, são definidos:

1. Burst de acesso: Esse burst é enviado pelo celular em um canal dedicado logo que ele procura entrar em contato com a rede para o estabelecimento de uma comunicação ou para um handover. Ele é o mais curto dos bursts e contem 77 bits (41 bits de sincronização e 36 bits de informação). Seu tempo de guarda é de 68.25 bits, ou seja, 0.252 ms, permitindo ter-se em conta as grandes células e estabelecer assim uma comunicação com um celular até 35 km de distancia. Calculando a duração de viajem do burst, a estação pode fixar o instante do inicio da emissão para compensar o retardo introduzido pela propagação da onda.

2. Burst de sincronização: Esse burst contém 78 bits de informação sobre as freqüências que devem ser utilizadas e a localização (identidade da estação de base, zona e célula).

3. Burst de correção de freqüência: sendo o burst mais simples, contem 142 bits que servem para prevenir as possíveis interferências das freqüências vizinhas.

4. « dummy burst » :que são definido a partir de uma burst normal contendo no lugar de dados uma seqüência fixa que não transporta nenhuma informação. O "dummy burst" é usado pela estação de base quando ela quer emitir um sinal sem, contudo enviar informações. Para ser preciso, esse burst é composto de 2 blocos de 58 bits prefixados intercalados por seqüência de aprendizagem de 26 bits.

A Figura 59 abaixo mostra os vários tipos de burts:

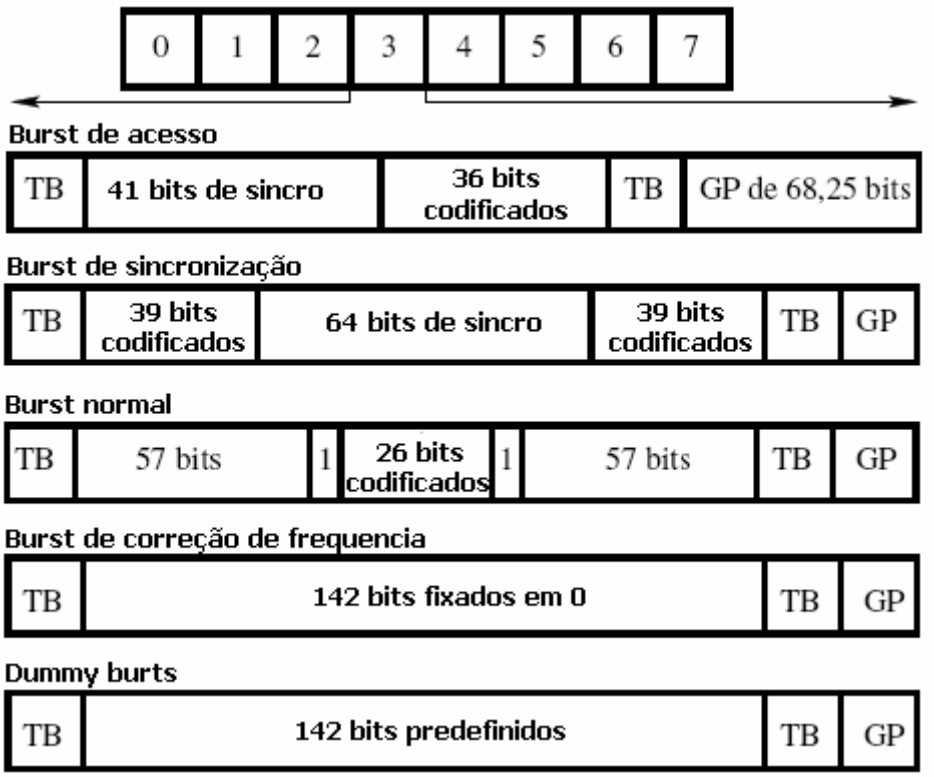


Figura 59 – Formato dos diversos burst GSM

Unidade 7 Canais Lógicos

A interface aérea permite interligar um usuário a rede celular. É necessário prevê funções de controle para que o celular se conecte a uma estação de base favorável a fim de estabelecer uma comunicação, supervisionar seu desenvolvimento e assegurar prováveis comutações de células (handover) ao longo da comunicação.

7.1 Estrutura da interface rádio

O serviço mais importante oferecido pelo GSM é o serviço de voz. O método mais simples para transmitir a voz é reservar canais de transmissão síncronos durante a duração de uma chamada. Esses canais são os canais de trafego TCH – Traffic Channel. Cada TCH ocupa um canal físico e corresponde a uma taxa de 13 kbis/s antes e de 22.8 kbis/s após a codificação do canal.

O GSM é um sistema de comutação de circuito. O BSC aloca um TCH a um celular que deseja comunicar da mesma maneira que uma central telefônica aloca um circuito para uma comunicação telefônica. Mas para funcionar, esse canal de trafego deve ser acompanhado de um certo número de canais lógicos de controle.

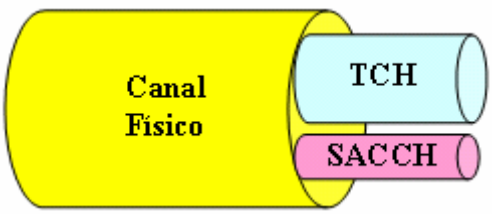
Para fazer comunicar duas entidades dentro de uma rede são necessários vários tratamentos e procedimentos que são classificados e colocados em camadas que se inspiram no modele OSI. As três camadas mais baixas 1,2 e 3 denominadas camada física, de enlace e de rede contem os elementos indispensáveis para assegurar a transmissão. A camada física que serve principalmente de modem numa rede clássica, no GSM compreende muitas funcionalidades tais como multiplexação, construção dos bursts, controle da potencia, controle do avenço do tempo TA, codificação/decodificação. Numerosos "fios" interligam a camada física a camada enlace. Eles correspondem ao sistema sofisticado de canais lógicos especifico ao contexto radio. A camada três é separada em varias subcamadas. Elas tratam os aspectos rede, aplicações telefônicas, tratamento das chamadas, serviços complementares, mensagens curtas.

7.2 Canais físicos e lógicos

Num par de freqüências, um slot particular dentre os oitos é alocado a uma comunicação com um dado celular. Esse par de slots forma um canal físico (duplex) que corresponde no caso a um circuito telefônico. Ele forma a base de dois canais lógicos:

TCH (Traffic Channel) – que transporta os dados digitais;

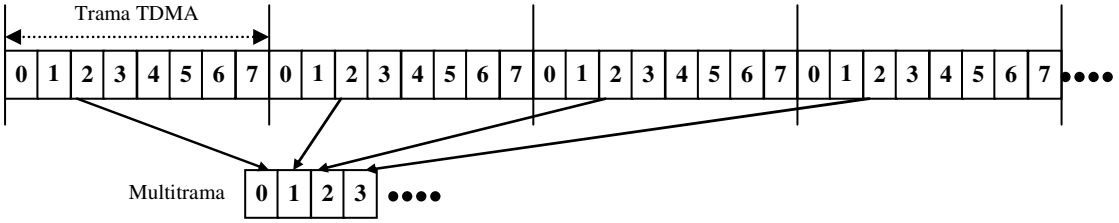
SACCH (Slow Associeted Control CHanne) – que permite controlar os parâmetros físicos da ligação.



Num sistema de comunicações móveis tal como o GSM é necessário prever na interface aérea um serie de funções de controle tais como:

- - difundir informações do sistema (Broadcast Channels);
- - prevenir aos celulares de chamadas chegando e facilitar seu acesso ao sistema (Commom Control Channels).
- - controlar os parâmetros físicos antes e durante as fases ativas de transmissão (FACCH, SCH e SACCH);
- - fornecer suporte para as transmissões de sinalização telefônica (SDCCH).

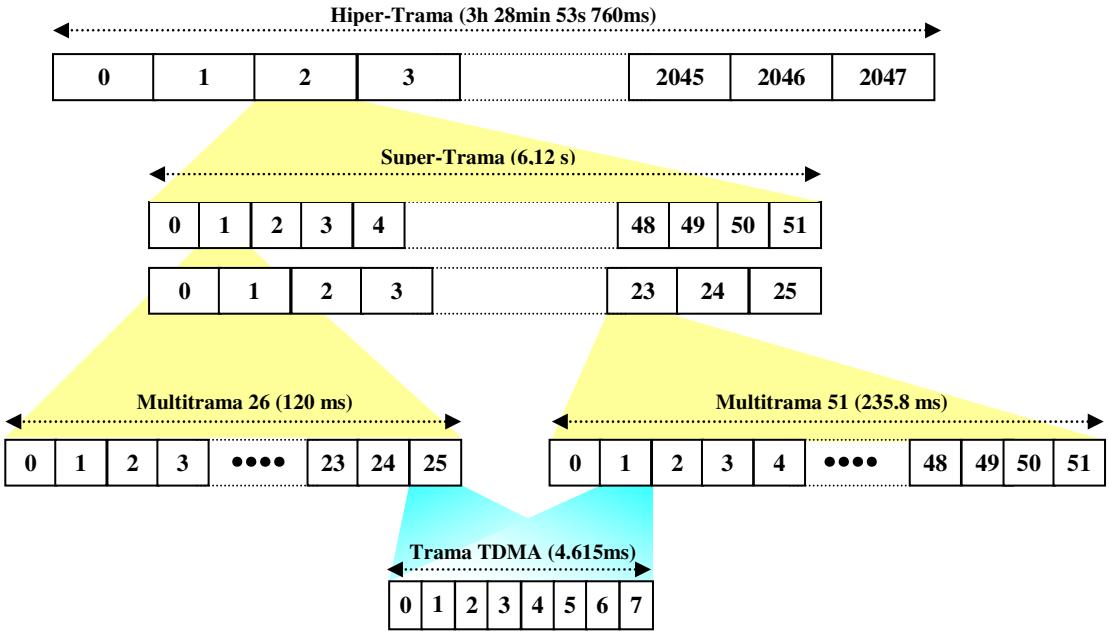
Para cada função necessária o sistema poderia utilizar um canal físico. Entretanto, isso seria um desperdício de recursos que são raros e caros. A fim de alocar o menor numero possível de slots por trama o sistema GSM define uma estrutura chamada de multitrama. Essa estrutura é definida por uma sucessão de um dado slot de tramas TDMA sucessivas (isto é, canais físicos). Entre dois slots de uma multitrama se passam 4.615 ms.). A figura abaixo mostra a estrutura de uma multitrama definida pelo slot 2 de cada trama TDMA.



O conjunto de slot dentro da multitrama permite transportar com uma periodicidade bem definida um certo tipo de informações de controle ou de sinalização. Esse conjunto de slot forma o "canal lógico". Os canais lógicos permitem economizar recursos na utilização da interface rádio, pois limitam os esforços de pooling dos equipamentos da rede Por exemplo, um celular deve constantemente escutar as informações transmitidas pela estação de base. Para evitar que o telefone celular análise escute todos os slots de todas as tramas, o GSM determina para cada slot de uma multitrama uma função bem especifica.

7.3 Estrutura temporal da multitrama

A figura abaixo mostra estruturação das tramas no sistema GSM.



A norma GSM define duas estruturas diferentes de multitramas. A primeira multitrama é composta de 26 tramas com uma duração total de 120 ms enquanto a segunda é composta de 51 tramas com uma duração total de 235.8 ms. Para dispor de uma estrutura comum aos dois tipos de multitramas o GSM define uma supertrama composta de 26 multitramas de 51 tramas ou de 51 multitramas de 26 tramas. Uma hipertramas é estão definida como sendo o conjunto de 1024 supertramas. Dessa forma uma hipertrama esta composta de 26 vezes 51 vezes 1024 tramas TDMA (ou seja, 2.715.648 tramas) e tem a duração total de 3h 28min 53s 760ms. Cada trama TDMA é identificada por um contador FN (Frame Number) dentro da hipertrama. A BTS transmite regularmente ao celular o contador FN permitindo de se localizar dentro da hipertrama.

O contador FN pode ser considerado como uma base de tempo própria da BTS sendo usado mesmo como parâmetros para algoritmo de criptografia A5.

7.4 Classificação dos canais lógicos

Existem duas classes de canais lógicos: os canais dedicados e os canais não dedicados.

Um canal dedicado fornece um recurso reservado a um celular. A um celular se atribui dentro da estrutura da multitrama um par de slots (um para recepção e outro para transmissão) nos quais somente esse celular poderá transmitir e receber. Dentro da mesma célula nenhum outro celular poderá transmitir ou receber no mesmo slot da mesma freqüência. Os canais dedicados são, portanto duplex.

Um canal não dedicado é simplex e compartilhado por um conjunto de celulares. No sentido descendente (DOWN), isso significa que os dados enviados nesse canal são difundidos e lidos por vários celulares que escutam esse canal. Esses dados podem ser dados do sistema ou de celulares que estão sendo chamados e que não tem ainda canais dedicados. No sentido ascendente (UP) o canal não dedicado permite a execução da função de acesso múltiplo (Random Access). Isso quer dizer que os celulares utilizam esses canais para enviar seus pedidos de acesso à rede.

A tabela abaixo resume os canais lógicos do GSM. As duas primeiras classes agrupam os canais não dedicados enquanto as outras duas agrupam os canais dedicados.

Broadcast Channel (BCH ↓) (unidirecional em difusão)	Frequency Correction Channel (FCCH) ↓	*Identificação da freqüência portadora*
	Synchronization Channel (SCH) ↓	*Sincronização e Identificação*
	Broadcast Control Channel (BCCH) ↓	*Informações do sistema*
Common Control Channel (CCCH ↓↑) acesso compartilhado	Paging Channel (PCH) ↓	*Chamado do celular*
	Random Access Channel (RACH) ↑	*Acesso aleatório do celular*
	Access Grant Channel (AGCH) ↓	*Alocação de recursos*
	Cell Broadcast Channel (CBCH) ↓	*Difusão de mensagens curtas*
Dedicated Control Channel (DCH ↓↑)	Stand-Alone Dedicated Control Channel (SDCCH) ↓↑	*Sinalização*
	Slow Associated Control Channel (SACCH) ↓↑	*Supervisão da ligação*
	Fast Associated Control Channel (FACCH) ↓↑	*Execução do handover*
Traffic Channel (TCH ↓↑)	Traffic Channel for speech (TCH/FS) e (TCH/HS) ↓↑	*Voz plena taxa/meia taxa*
	Traffic Channel for data ↓↑	*Dados do usuário*

7.5 Canais dedicados

7.5.1 TCH e SDCCH

Existem os canais dedicados que transportam informações do usuário e os que transportam informações vindas das aplicações do sistema. São respectivamente os canais de trafego TCH (Traffic Channel) e os canais de sinalização SDCCH (Stand-alone Dedicated Control CHannel). O TCH permite a transmissão de voz a 13 kbits/s e de dados em até 12

kbits/s, enquanto o SDCCH utiliza uma taxa de transmissão de 0.8 kbits/s. Um SDCCH pode ser visto como um TCH de tamanho reduzido para a sinalização.

Em um canal físico podemos ter um canal TCH ou 8 canais SDCCH. Isso nos leva a deduzir que um SDCCH = TCH / 8.

7.5.2 Canal SACCH

Uma conexão rádio é flutuante, não sendo possível de dedicar um canal a um celular sem controlá-lo em permanência. É necessário constantemente ajustar parâmetros para conservar uma qualidade de serviços aceitável. A rede também deve verificar se o celular permanece ativo no canal. Para isso, os canais dedicados TCH e SDCCH possuem cada um um canal de controle associado de baixa taxa chamado SACCH (Slow Associated Control Channel). A SACCH suporta as informações seguintes:

- - compensação do atraso de propagação ida-volta (round trip delay) para o mecanismo de avanço do tempo;
- - controle da qualidade da conexão rádio;
- - medidas efetuadas nas estações vizinhas.

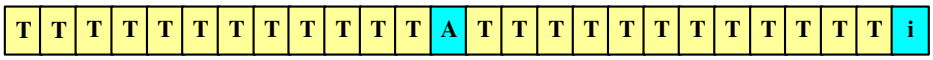
Um SACCH transporta as informações em 184 bits úteis que protegidos formam um bloco de 456 bits transportados em 4 burst normais.

7.5.3 Multiplexagem TCH-SACCH

Uma estação móvel em comunicação precisa de um par de slots por trama para comunicar. O codificador de voz envia a cada 20ms um conjunto de 260 bits que são protegidos e agrupados em um bloco de 456 bits. Um bloco de 456 bits de voz é enviado em 4 burst, sendo que cada burts deveria ser enviada em um tempo de 5ms. Entretanto a trama GSM é mais curta e dura exatamente 5*(24/26) ms, ou seja, 4.61538ms. Durante um período de 120ms (6 blocos de voz) 24 burst de voz são utilizados. Como o celular dispõe de 26 slots (120 / 4.61538) ficam entao 2 slots livre. Um slot é utilizado para o canal SACCH e o outro é chamado de idle ou "slot de repouso". O celular utiliza esse slot para "escutar" as freqüências balizas das estações vizinhas.

Esta estrutura se repete a cada 120ms, ou seja, todas as 26 tramas TDMA (multitrama a 26 tramas). O slot 12 é alocado para o canal SACCH e o slot 25 é o slot idle.

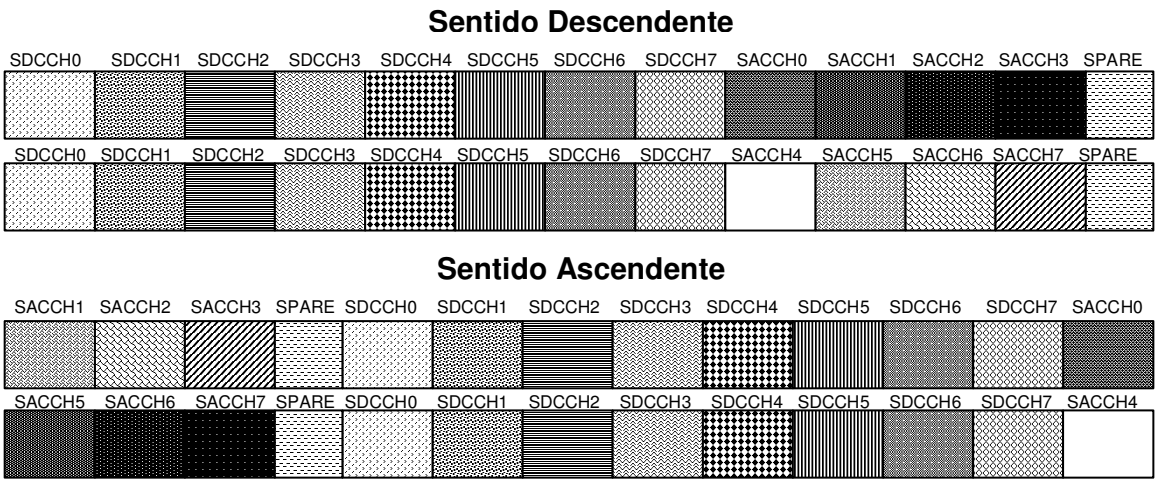
Multitrama a 26 tramas



A – SACCH T – TCH i – IDLE

7.5.4 Multiplexagem SDCH-SACCH

Um SDCCH e seu SACCH são multiplexados em um mesmo canal físico duplex com outros pares SDCCH-SACCH. A estrutura utilizada repousa sobre um multitrama a 51 tramas. Cada SACCH ocupa 4 slots consecutivos do canal como pode ser vista na figura abaixo. Os slots 32 a 47 são utilizados nas multitramas pares para os canais associados aos canais SDCCH 0, 1, 2 e 3. Nas multitramas impares esses slots são usados para os canais SDCCH 4, 5, 6 e 7. A figura abaixo mostra a distribuição normalmente utilizada dos canais SDCCH e SACCH no canal físico 1 da freqüência baliza.


Sentido Descendente
SDCCH0 SDCCH1 SDCCH2 SDCCH3 SDCCH4 SDCCH5 SDCCH6 SDCCH7 SACCH0 SACCH1 SACCH2 SACCH3 SPARE
SDCCH0 SDCCH1 SDCCH2 SDCCH3 SDCCH4 SDCCH5 SDCCH6 SDCCH7 SACCH4 SACCH5 SACCH6 SACCH7 SPARE
Sentido Ascendente
SACCH1 SACCH2 SACCH3 SPARE SDCCH0 SDCCH1 SDCCH2 SDCCH3 SDCCH4 SDCCH5 SDCCH6 SDCCH7 SACCH0
SACCH5 SACCH6 SACCH7 SPARE SDCCH0 SDCCH1 SDCCH2 SDCCH3 SDCCH4 SDCCH5 SDCCH6 SDCCH7 SACCH4

7.6 Canais não dedicados

7.6.1 O conceito de canal baliza

Uma das funções primordiais em um sistema celular é aquela que permite ao celular de se conectar permanentemente à estação de base mais favorável. Essa função é realizada graças ao canal baliza (beacon channel) próprio a cada estação de base. O canal baliza de uma BTS corresponde a uma freqüência particular pertencente ao conjunto de freqüências alocadas à estação. Um celular da vizinhança mede periodicamente neste canal o nível de sinal que ele recebe. Ele determina através dessa medida de potencia se ele esta ao alcance da estação e se ele esta próximo ou distante da BTS. Cada canal baliza compreende igualmente sinais de forma específica e informações do sistema. Os sinais permitem ao celular detectar a presença da estação de base e se localizar em freqüência e em tempo. As informações do sistema correspondem à identificação da rede e suas características de acesso.

Ao ser colocado no estado ligado, o celular procura se localizar no canal baliza da BTS mais favorável pertencente a sua rede PLMN. Ele então observa constantemente o sinal recebido neste canal bem como o sinal recebido no canal baliza das BTS vizinhas. Desde que necessário, ele se localiza num novo canal mudando assim de célula. Da mesma maneira, um celular em comunicação escuta periodicamente as estações das células vizinhas construindo uma lista de estações favoráveis a um provável handover.

O canal baliza de uma estação de base corresponde aos dois elementos seguintes:

- - uma freqüência descendente na qual é emitido em permanência um sinal modulado de potencia constante que permite aos celulares fazer medidas de potencia;
- - um conjunto de canais lógicos em difusão implantados nesta freqüência principalmente no slot 0 (zero).

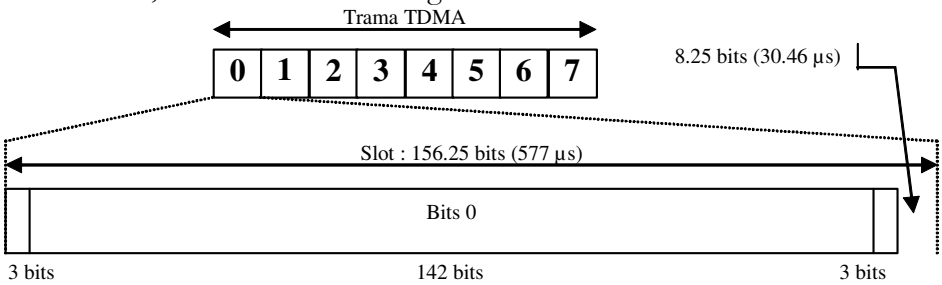
A freqüência baliza é escolhida entre o conjunto de portadoras atribuídas ao operador. Ela suporta também um certo numero de canais dedicados num mínimo de 4 (nos slots 1, 3, 5 e 7) e num máximo de 7 (só o slot 0 é dedicado ao controle comum).

Os canais lógicos em difusão permanente permitem a cada celular de se conectar ao sistema para receber os parâmetros lógicos necessários. São eles:

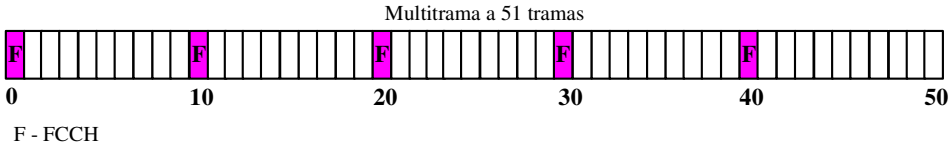
- - canal FCCH (Frequency Correction CHannel) para a sincronização em freqüência;
- - canal SCH (Synchronisation CHannel) para a sincronização em tempo;
- - canal BCCH (Broadcast Control CHannel) para a difusão de informações.

7.6.2 Canal FCCH

O canal FCCH consiste de um burst particular emitido a cada 50ms, aproximadamente. Esse burst é composto de 148 bits zeros (senoide perfeita) que permitem uma sintonização fina do oscilador do celular, conforme mostra a figura abaixo.



O canal FCCH esta presente somente no slot 0 (zero) da freqüência baliza, sendo emitido nas tramas 0, 10, 20, 30 e 40 de uma supertrama de 51 tramas. Isso significa que ele é emitido 5 vezes a cada 235.8 ms, isto é, 20 vezes no segundo. A figura abaixo mostra o uma supertrama de 51 tramas e a localização dos canais FCCH.



7.6.3 Canal SCH

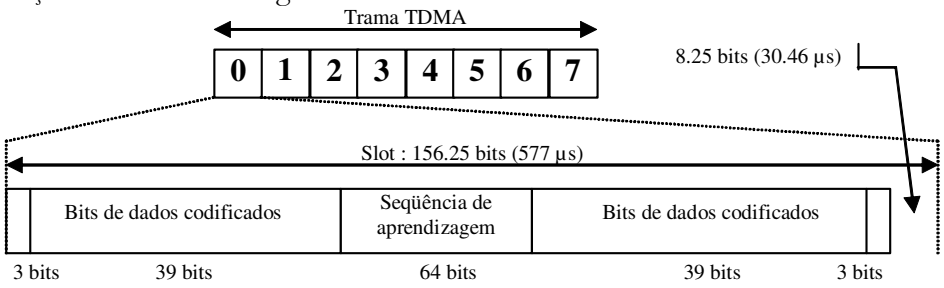
O canal SCH (Synchronisation CHannel) tem por objetivo fornecer aos celulares os elementos necessários a uma completa sincronização. Ele permite também caracterizar a via baliza por uma marcação especial que não é encontrada em nenhum outro canal físico. Essa marcação é a seqüência de aprendizagem de 64 bits.

Dois níveis de sincronização podem ser distinguidos:

- a sincronização fina - ajuda na determinação do TA;
- a sincronização lógica – determinação do FN, que consiste de colocar o contador FN do celular em fase com o contador da BS.

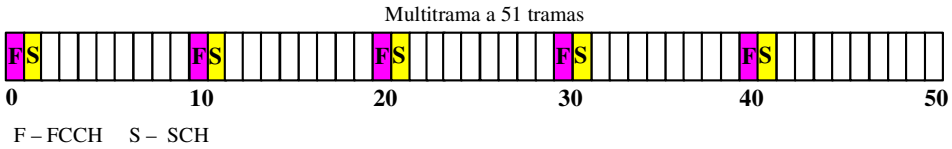
7.6.3.1 Estrutura do burst

O burst presente no SCH é composto de uma seqüência de aprendizagem e de 78 bits de dados codificados. A seqüência de aprendizagem é composta de 64 bits (mais longa que a de um burst normal) para permitir ao celular fazer uma analise fina do canal e de se sincronizar com a estrutura TDMA da estação de base. Essa seqüência é comum a todas as estações de base de todas as redes PLMN porque o burst do SCH é o primeiro que uma celular decodifica para extrair as informações transmitidas logicamente.



7.6.3.2 Colocação do SCH na trama TDMA

O burst SCH só é enviado no slot 0 de uma trama TDMA. Ele é sempre situado na trama após o burts FCCH. Após a sincronização em freqüência o celular tenta decodificar esse burts para ter a certeza que a freqüência que ele escuta é mesmo a baliza de uma estação de base GSM.



7.6.3.3 Sincronização fina

Essa sincronização é de natureza física. Para o celular, ela consiste em efetuar uma sincronização precisa em tempo logo que ele detecta e analisa a seqüência de aprendizagem do burst SCH.

7.6.3.4 Dados transportados

O canal SCH transporta em cada burst dois parâmetros de 25 bits:

- - o numero da trama reduzido RFN (Reduced TDMA Frame Number) de 19 bits que permite determinar o FN (Frame Number);
- - o código de cores BSIC de 6 bits que permite diferenciar estações de base pouco afastadas que utilizam a mesma freqüência baliza.

Aos 25 bits úteis são ao acrescentados 14 bits (10 de CRC e 4 de marca) formando um bloco de dados de 39 bits. A esse bloco de bits são aplicados códigos de correção de erros totalizando 2 vezes 39 bits, ou seja, 78 bits de dados.

7.6.3.5 Sincronização Lógica

O numero FN é definido pelo modulo M = 26 * 51 * 2^11 sendo necessário $\log_2(M)$ bits, ou seja, 22 bits para representá-lo. O numero da trama RFN difundido no canal SCH composto de 19 bits possui os seguintes campos:

- - 11 bits que codificam o numero da super-trama corrente com relação à hiper-trama;
- - 5 bits que codificam o numero da multi-trama a 51 tramas com relação a super-trama;
- - 3 bits que determinam a trama corrente dando o lugar do canal SCH dentre os 5 possíveis na multitrama (1, 11, 21, 31 ou 41). Essa solução economiza 3 bits, já que par codificar o numero do SCH seriam necessários $\log_2(51)$ bits, ou seja, 6 bits.

A recepção do SCH permite ao celular calcular o numero da FN dentro da hipertrama e de se localizar sobre o slot 0, ficando assim sincronizado com a BTS.

7.6.3.6 Código de cores BSIC (Base Station Identity Code)

A mesma freqüência pode ser utilizada como freqüência baliza de duas BTS suficientemente distantes uma da outra. As duas estações não se interferem dentro de suas zonas de serviços, entretanto um celular situado a meia distancia delas pode receber uma e outra estação com um nível de sinal considerável. Será necessário então diferenciar as duas estações por uma informação especifica. Para isso utilizamos o código de cores composto de dois campos:

- - 3 bits para o código da cor da estação de base dentro da PLMN;

- - 3 bits para o código da cor de uma PLMN.

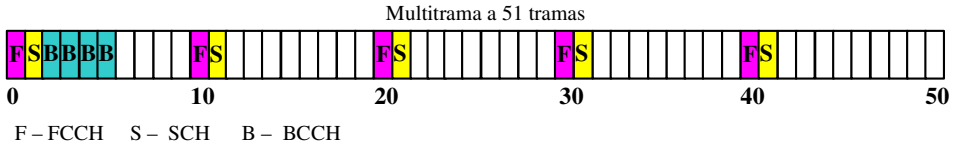
7.6.4 Canal BCCH

O BCCH (Broadcast Control Channel) é utilizado para difundir os parâmetros lógicos característicos (ou informações do sistema) das células. Essas informações são agrupadas em 184 bits úteis que são codificas em um bloco de 456 bits e enviadas em 4 burst normais. O canal BCCH é enviado a uma taxa de 782 bits/s.

As informações contidas no BCCH são as seguintes:

- - os parâmetros para seleção de células (nível mínimo de sinal exigido, nível Maximo de potencia autorizado);
- identificação (numero) da zona de localização ou LAI;
- os parâmetros que dão as regras de acesso aleatório (RACH);
- a descrição da organização dos canais de controle comuns.
- a descrição da organização do canal CBCH (Cell Broadcast CH);
- as freqüências balizas das células vizinhas (descrição das células vizinhas);
- a lista das portadoras do BTS;
- a identificação da célula (BSIC);
- outros parâmetros necessários (controle de potencia, etc).

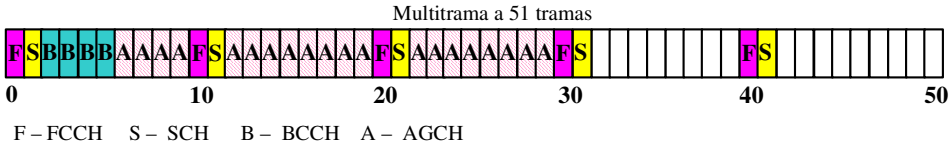
O canal BCCH se encontra no slot 0 da freqüência baliza. Entretanto canais suplementares podem ser utilizados nos slots 2,4 e/ou 6. A figura abaixo mostra a localização normal do canal BCCH.



7.6.5 Canal AGCH

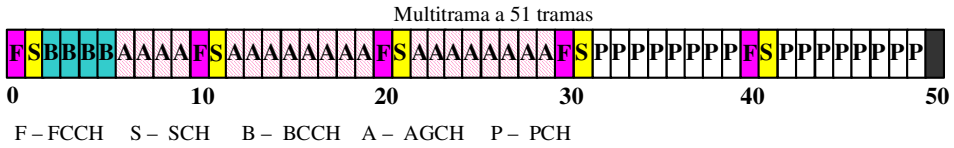
Logo que a rede recebe uma solicitação de um celular é necessário alocar um canal de sinalização para identificar o celular, autenticá-lo e determinar qual é precisamente sua solicitação. A alocação de dum canal dedicado é feita através de slots predefinidos que formam o canal AGCH (Access Grant Channel).

A mensagem de alocação contém a descrição completa do canal de sinalização utilizado: numero da portadora, numero do slot, descrição do salto de freqüência se implantado e o parâmetro TA. A mensagem de alocação é formada por 23 bytes, codificados e enviados em 4 burts normais.



7.6.6 Canal PCH

Logo que a rede deseja comunicar com o celular para uma chamada, um SMS ou uma autenticação ela difunde a identidade do celular em um conjunto de células da LA transmitindo a mensagem em um canal PCH (Paging CHannel).O celular responde utilizando o canal RACH.Uma ou mais mensagens de chamada em difusão podem ser incluídas em uma palavra de 23 bytes, codificada e enviada em 4 bursts normais. É possível chamar em difusão até 4 celulares utilizando-se o TMSI que é menor que o IMSI.



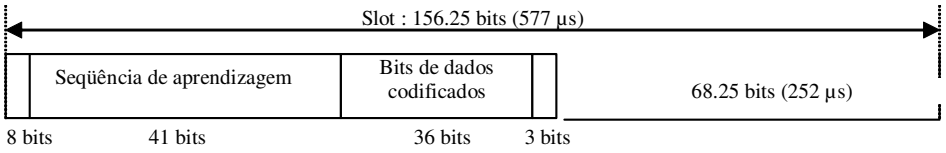
7.6.7 Canal RACH

Par cada ação tais como localização, SMS e chamadas o celular deve sinalizar e rede. Para isso ele envia uma mensagem muito curta em um só burst para a BTS. A mensagem é enviada em slots particulares de acesso à rede chamados RACH (Random Access CHannel).

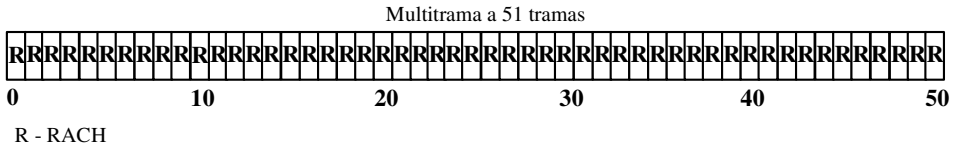
O burts RACH é mais curto que o burst normal porque o celular não conhece o atraso de propagação entre o lugar onde ele se encontra e a BTS. O burst emitido deve se inserir completamente dentro do slot da BTS sem se superpor com outros slots vizinhos. O tempo de guarda é então de 252 us permitindo ao celular estar até 37,8Km afastado da BTS.

A seqüência de sincronização é composta de 41 bits para permitir a estação de base detectar o sinal do celular que não está ainda totalmente sincronizado.

O canal RACH contem 8 bits úteis protegidos por 6 bits de CRC. A esses bits são acrescentados 6 bits do código BSIC que permitirão a BTS verificar se o burst foi realmente a ela endereçado. Após a aplicação do código de proteção o burst conterá 36 bits de dados. O formato do burts é mostrado na figura abaixo.

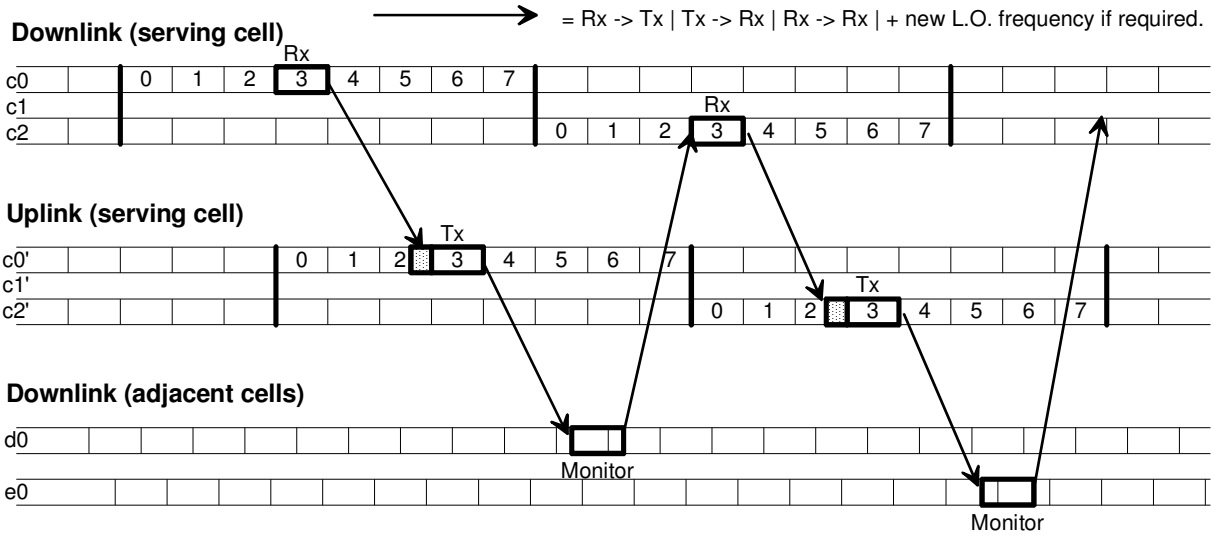


A figura abaixo mostra a localização do canal RACH no slot 0 da freqüência baliza no sentido uplink.



7.7 Monitoramento

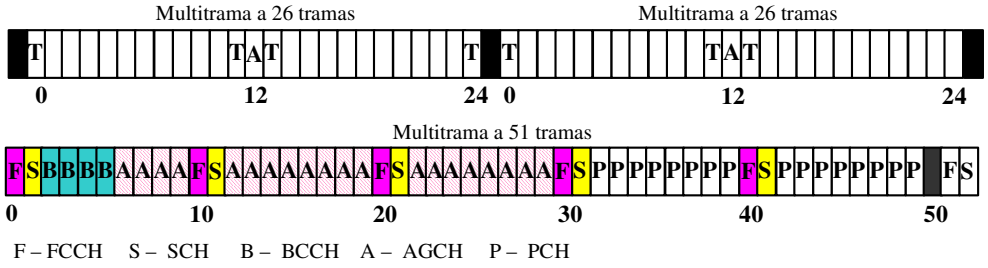
Durante uma comunicação o celular não se contenta só de receber e transmitir tramas. Ele utiliza o tempo compreendido entre a emissão e a recepção de um burst para “escutar” a as freqüências das células vizinhas e fazer as medidas necessárias.



7.7.1 Monitoramento nas multitramas a 26 e a 51

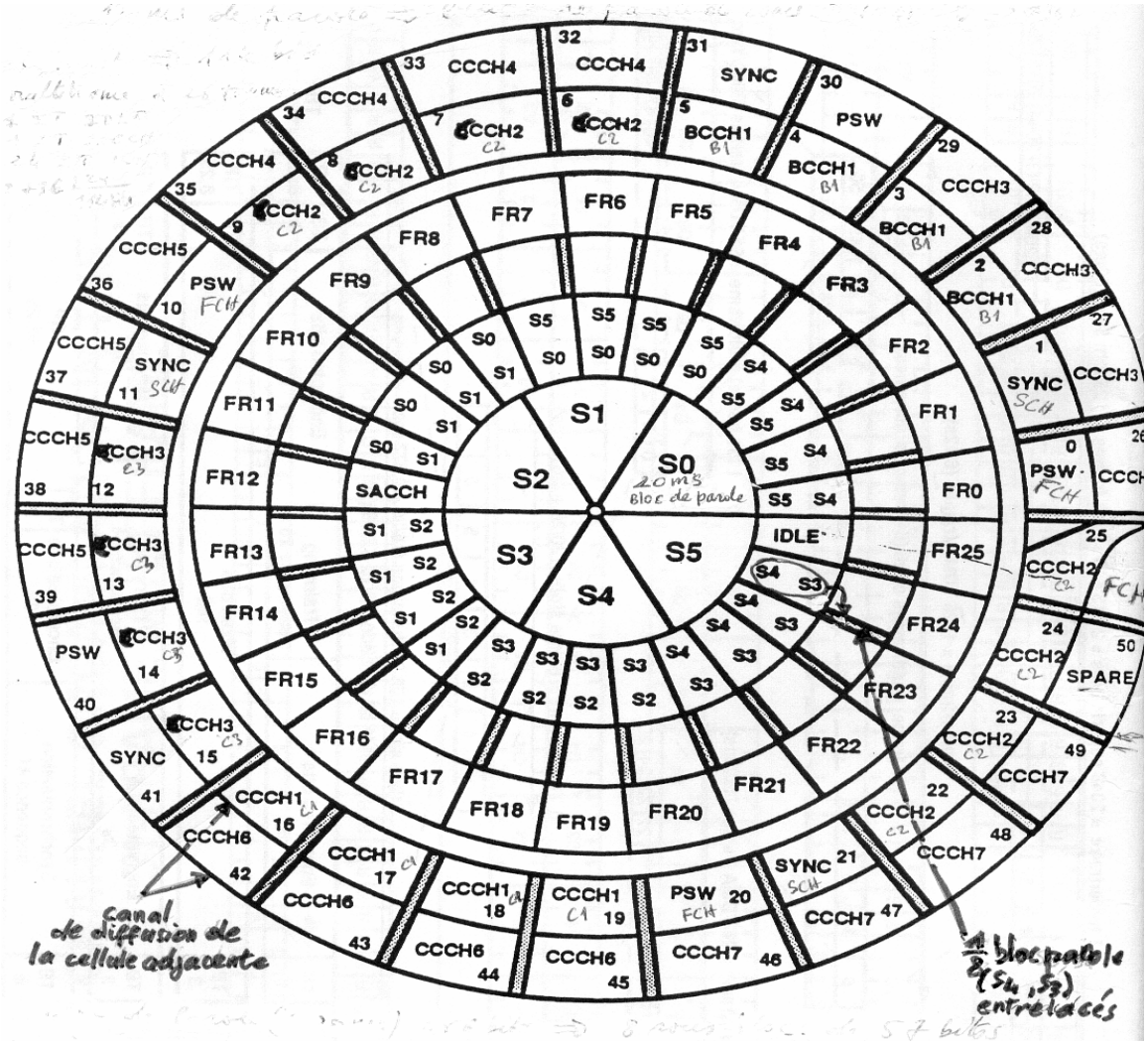
Quando um celular está em comunicação utilizando um TCH ele transmite e recebe sobre um slot particular da multitrama a 26. Entretanto, o 26º slot é o slot idle onde o celular nem transmite nem recebe.

O conjunto de canais em difusão é transmitido numa estrutura a 51 trama. Sendo os numero 26 e 51 primos entre si, a janela de observação do celular vai deslizar com relação a estrutura a 51 tramas. Se a um momento o celular lê o slot 0 da trama 0 do trama a 51, nas janelas de observação seguinte ele vai ler o slot 0 da trama 26, 1, 27, 2, 28, etc. Um celular é então capaz de receber os canais FCCH e SCH de todas as estações vizinhas, a condição que o sinal seja de qualidade suficiente para a decodificação. Como as informações necessárias a sincronização são transmitidas em um só burst do canal SCH, fica assim assegurada a aquisição das informações de sincronização das estações vizinhas por parte do celular.



7.8 Hypertrama

- - 1 Hypertrama = 2048 Supertramas = 2715648 tramas TDMA ⇒ 3H28mn760s
- - 1 Supertrama = 51multitramas à 26 tramas = 26 multitramas à 51 tramas = 1326 tramas TDMA ⇒ 6mn12s
- - 1 Multitrama à 26 trames = 26 tramas TDMA ⇒ 120 ms
- - 1 Multitrama à 51 tramas = 51 trames TDMA ⇒ 3060/13 ms
- - 1 Trama TDMA = 8 IT (Time Slots) ⇒ 120/26 = 4,61538 ms
- - 1 Time Slot (TS) = 156,25 durações ⇒ 15/26 = 0,577 ms
- - 1 duracao de bit ⇒ 48/13 = 3,69 µs
- - Tipos de Burst : Normal Burst (NB), Frequency correction Burst (FB), Synchronisation Burst (SB), Access Burst (AB), Dummy Burst (DB).



7.8.1 Características dos Canais GSM

Tipo	Bits Úteis (bits)	Bits Total (bits)	Taxa (kbit/s)	Periodicidade (ms)
TCH	260	456	13	20
TCH/9.6	4*60	456	9,6	20
SACCH(TCH)	184	456	0,382	480
SDCCH	184	456	0,782	235,8
SACCH(S)	184	456	0,391	471,6
FCCH	0			
SCH	25	78		
BCCH	184	456	0,782	235,8
PCH+AGCH	184	456		
RACH	8	36		